COBIT® e sistema di controllo interno nella Legge 262/2005

PREFAZIONE

COBIT® e il sistema di controllo interno nella Legge 262/2005

L'obiettivo assegnato dal Direttivo AIEA al Gruppo di Ricerca è stato l'emanazione di un Documento Aiea che definisca le linee guida ed i modelli di riferimento al fine di giungere alla conformità legislativa prevista dalla Legge 262/2005 a fronte dei controlli relativi alla componente tecnologica.

La ricerca è stata scomposta in un certo numero di tematiche ognuna di esse assegnata ad un Focus Group. La distribuzione delle tematiche è stata la seguente:

Focus Group 1:
Tematiche:

- **utilizzabilità ed adattabilità** alla normativa italiana del documento *"IT Control Objectives for Sarbanes-Oxley"* edito dall'ITGI ® v2.
- **differenze** con altre normative internazionali (S&O Act – Section 404, JSOX, ecc…)
- caratteristiche generali di un **Framework** di controllo
- Richiamo di fonti comparative di interesse in ambito Legge 262/2005 e IT controls

Focus Group 2:
Tematiche:

- Adozione di un **Risk Based** Approach
- Collegamenti ad **altri modelli aziendali** di Governance e Risk Management
- Individuazione del **perimetro di applicazione** (perimetro delle entità legali e ambiti IT delle stesse)

Focus Group 3:
Tematiche:

- **Entity** (o Company) Level Controls (ELC o CLC)
- IT **General** Controls (o controlli generali IT o GCC)
- Service Provider
- End User Computing

Focus Group 4:
Tematiche:

- **Application** Controls;
- **Segregation of Duties;**

- Obiettivi / rischi per **settore industriale**

Focus Group 5:
Tematiche:

- Metodi di **testing** e **campionamento**
- **Frequenza** del testing e **monitoraggio** dei controlli
- Modalità di **documentazione** dei controlli IT (evidenza e conservazione)

Focus Group 6:
Tematiche:

- **Flussi interni di attestazione** tra IT e Dirigente preposto
- **Modello finale di valutazione** del sistema di controllo interno
- **Mantenimento/efficientamento** della compliance nel tempo

Fermo rimanendo lo schema dei contenuti sopra descritti, nel corso dello svolgimento del lavoro il Gruppo di Ricerca ha ritenuto di poter procedere alla pubblicazione dei primi 5 studi al fine di rendere disponibile alla compagine dei soci AIEA un primo importante quadro omogeneo di riferimento della materia, affidando ad una successiva versione gli approfondimenti tecnici del campionamento (Focus Group 5) e della identificazione dei rischi per settori industriali richiamati nell'ambito del Focus Group 4.

Per ciascun Focus Group il controllo di qualità è stato svolto da un socio di altro Focus Group che ha effettuato una rilettura critica del materiale prodotto. Referente del Consiglio Direttivo AIEA per il coordinamento complessivo della ricerca è stato Enzo Toffanin.

Autori della ricerca sono pertanto i 14 soci partecipanti ai 5 Focus Group a cui va il ringraziamento di AIEA per la fatica compiuta.

I partecipanti al GdR sono stati:

Alessandro Arca, Fiatrevi SpA
Emanuele Boati, Unicredit Group
Alessandro Crestani, Intesa Sanpaolo
Giuliano Flesia, Intesa Sanpaolo
Alfredo Gallistru, Price Waterhouse Coopers
Massimiliano Motta, UBI Banca
Leonardo Nobile, Deloitte
Luca Nurisso, Fiat SpA
Franco Orsogna, Deloitte
Giandomenico Palumbo, E&Y
Dino Ponghetti, Price Waterhouse Coopers
Mihaela Simona Popa, Unicredit Audit
Marco Salvato, Generali Business Solutions
Luca Turri, Intesa Sanpaolo
Marcello Zerboni, Telecom Italia

INTRODUZIONE

Documento di Ricerca AIEA
COBIT® e controllo interno nella Legge 262/2005

Destinatari di questa guida sono i soggetti a cui si applica la Legge 262/2005. Si tratta delle società quotate, quotande e le società che abbiano volontariamente scelto di applicare la norma. Ma più in generale le società ove il controllo interno sia oggetto di esplicita gestione e monitoraggio secondo modalità stabilite dall'Alta Direzione, ancorchè non siano formalmente sottoposte alla disciplina, potranno trovare in questo scritto una utile guida.

Il perimetro oggetto dei controlli trattati in ambito Legge 262/2005 è quello dei controlli finalizzati alla formazione del bilancio (ovvero Internal Controls over Financial Reporting, adottando la terminologia internazionale). Questa delimitazione applicata al mondo dei controlli sui sistemi informativi ha comportato un intenso dibattito fra gli addetti in quanto ha introdotto una breccia nel principio che i processi che alimentano la produzione informatica sono tutti (nessuno escluso) concorrenti alla affidabilità dei risultati per gli utenti. Concetto, questo, teoricamente corretto, ma incerto nella sua pratica applicazione. Una debolezza in un controllo è rilevante ai fini del controllo interno come disciplinato nella Legge 262/2005 se di essa si riesca a comprendere l'impatto sulla formazione dei dati contabili e in ultima istanza del bilancio. Ai fini della produzione del Bilancio (Financial Reporting) questa relazione di causa ed effetto ha comportato una delimitazione del più generale complesso dei controlli sui processi informatici ad un sottoinsieme "rilevante" ai fini sopraddetti. Tale delimitazione è particolarmente espressa nel documento "IT Control Objectives for Sarbanes Oxley" (ITGI 2006).

La presente Guida ha coordinato in un unico documento, utile sia per il Management sia per l'Audit Interno, la lettura di varie fonti utilizzate nella pratica in sede di definizione dei controlli interni e della loro verifica di operatività.

Nella formulazione dei controlli data dalle aziende e dai loro consulenti la pratica è generosa di una varietà di modalità espressive dei controlli frutto della storia individuale e delle conoscenze professionali proprie. Utile in questa varietà di approcci è trovare un denominatore comune come architettura complessiva del sistema di controllo. Ciò significa che, fatto salvo il dettaglio dei controlli che di necessità sarà aderente alla tipologia del business e alle caratteristiche quali-quantitative dell'organizzazione aziendale, gli elementi costituenti il sistema di controllo interno IT nel suo complesso, in una parola il "framework", devono essere riconoscibili e condivisi dalla generalità degli esperti del settore. Su questa linea la Guida porta il proprio contributo dando una lettura di ITGI "Control Objective for Sarbanes Oxley" ragionata e coordinata con l'esperienza pratica. Da ultimo la Guida fornisce un parametro utile per la comprensione del sistema di controllo adottato, la sua valutazione di efficacia quanto più possibile oggettiva, la sua confrontabilità (benchmarking) come stimolo al miglioramento continuo.

Enzo Toffanin

INDICE

1 COBIT® E Legge 262/2005 - QUADRO NORMATIVO

(FOCUS GROUP 1)

1.1 Presupposti e quadro di riferimento

1.1.1 Il quadro normativo

Con l'introduzione della **Legge 28 dicembre 2005, n. 262** in materia di "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari", entrata in vigore il 12 gennaio 2006, è stato disposto un rafforzamento della responsabilità delle aziende e della tutela del risparmio investito in strumenti finanziari; in analogia a quanto avvenuto nel contesto internazionale anche a seguito di rilevanti episodi fraudolenti.

La legge sul risparmio affronta le problematiche dei mercati finanziari e in particolare i temi della *Corporate Governance*, della disciplina delle società estere, delle norme europee sui prospetti informativi, dei conflitti di interesse degli intermediari, della regolamentazione delle attività svolte dalle Società di revisione, della distribuzione di compiti tra le Authority e delle disposizioni sul falso in bilancio.

In questo ambito la legge (Titolo 1 – Capo III – Sezione V bis – Art. 154bis), con riferimento agli emittenti quotati aventi l'Italia come Stato membro di origine, introduce la figura del "**dirigente preposto** alla redazione dei documenti contabili societari".

> Art. 154-*bis*. - *(Dirigente preposto alla redazione dei documenti contabili societari).*
>
> "*Gli atti e le comunicazioni della società diffusi al mercato e relativi all'**informativa contabile** anche infrannuale della stessa società sono accompagnati da una dichiarazione scritta del dirigente preposto alla redazione dei documenti contabili societari, che ne attestano la **corrispondenza alle risultanze** documentali, ai libri e alle scritture contabili."*
>
> *"Il Dirigente Preposto alla redazione dei documenti contabili societari predispone **adeguate procedure amministrative e contabili** per la formazione del bilancio di esercizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario."*

All'Amministratore (o Consigliere) Delegato e al Dirigente Preposto (di seguito DP) vengono quindi assegnate specifiche responsabilità funzionali a garantire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria della società. In particolare, è previsto che:

- il Dirigente Preposto debba predisporre adeguate procedure per la formazione del bilancio e di ogni altra comunicazione finanziaria (comma 3);

- l'Amministratore Delegato ed il Dirigente Preposto debbano attestare, con apposita relazione allegata al bilancio d'esercizio e consolidato annuale e al bilancio semestrale abbreviato (comma 5):

  a) l'adeguatezza e l'effettiva applicazione nel periodo delle procedure amministrative e contabili;
  b) la conformità dei documenti ai principi contabili IAS/IFRS emanati dallo IASB ed omologati dalla Commissione Europea;
  c) la corrispondenza dei documenti alle risultanze dei libri e delle scritture contabili;
  d) la loro idoneità a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria del Gruppo;
  e) che la relazione sulla gestione del bilancio d'esercizio e consolidato annuale comprende un'analisi attendibile dell'andamento e del risultato della gestione, nonché della situazione del Gruppo, unitamente alla descrizione dei principali rischi e incertezze cui quest'ultimo è esposto;
  f) che la relazione intermedia sulla gestione del bilancio semestrale abbreviato contiene un'analisi attendibile dell'incidenza degli eventi importanti che si sono verificati nei primi sei mesi dell'esercizio, unitamente a una descrizione dei principali rischi e incertezze per i sei mesi restanti dell'esercizio.

- il Dirigente Preposto debba attestare la corrispondenza alle risultanze documentali, ai libri ed alle scritture contabili degli altri atti e delle comunicazioni al mercato relativi all'informativa contabile (comma 2);

- l'Organo Amministrativo vigili affinché il Dirigente Preposto disponga di adeguati poteri e mezzi per l'esercizio dei compiti a lui attribuiti, nonché sul rispetto effettivo delle procedure amministrative e contabili (comma 4).

L'art. 154 bis è stato ispirato alla normativa introdotta negli USA dal Sarbanes Oxley Act. Rispetto a quest'ultima, la legislazione italiana non prevede peraltro l'obbligo di una relazione indipendente, da parte della Società di revisione, che attesti il disegno e l'efficacia operativa dei controlli.

1.1.2 Framework di riferimento

1.1.2.1COSO

Il riferimento utilizzato dal Legislatore alle "procedure amministrative e contabili", deve essere inquadrato nel più ampio concetto di "sistema di controllo interno".
Presupposto fondamentale per l'adeguatezza delle "procedure amministrative e contabili" è quindi l'istituzione ed il successivo mantenimento nel tempo di un adeguato sistema di controllo interno, in linea con un framework di riferimento comunemente accettato.
A tale riguardo il modello elaborato dal Committee of Sponsoring Organizations of the Treadway Commission (**COSO**), e accolto dal Codice di autodisciplina delle società quotate, rappresenta ad oggi il riferimento maggiormente utilizzato. I principi generali in esso descritti sono certamente utili per il DP.
Il modello pubblicato dal COSO nel 1992 (**Internal Control-Integrated Framework**) ha l'obiettivo di aiutare le aziende a valutare e a migliorare i propri sistemi di controllo interno.

Tale modello costituisce oggi uno standard di rilievo ed è utilizzato dal management delle società quotate negli Stati Uniti per adempiere alle disposizioni della sezione 404.

Secondo tale modello il sistema dei controlli interni è inteso come un processo che coinvolge tutte le funzioni aziendali, e che pertanto deve fornire ragionevoli assicurazioni circa il perseguimento degli obiettivi aziendali. In particolare:

- efficacia ed efficienza nella conduzione delle operazioni aziendali (operations);
- attendibilità dell'informazione finanziaria (reporting);
- conformità alle leggi e ai regolamenti in vigore (compliance).

Le attività operative sono intese come l'insieme dei processi operativi attraverso cui si sviluppa il business aziendale; il reporting è inteso come l'insieme dei processi di raccolta, elaborazione e pubblicazione delle informazioni di carattere economico-finanziario; la conformità alla normativa è l'osservanza da parte dell'impresa delle leggi e dei regolamenti ad essa applicabili.

A partire dal 2001 la crescente attenzione alla Gestione dei Rischi ha portato allo sviluppo di un framework di supporto per l'identificare e la gestione del rischio.

Nel mese di settembre 2004 il Committee Sponsoring Organizations of the Treadway Commission (COSO) ha pubblicato **l'Enterprise Risk Management (ERM) – Integrated Framework** con l'obiettivo di fornire un supporto alle aziende (September 29, 2004).

Il Sistema di Controllo Interno è parte integrante dell'Enterprise Risk Management – Integrated Framework; l'ERM contiene alcune sezioni dell'Internal Control-Integrated Framework e lo incorpora integralmente come riferimento.

Al fine di fornire alle società "non grandi" (**smaller company**) un orientamento sull'applicazione nella pratica del **COSO Framework** è stata predisposta dal COSO nel 2006 una guida per aiutare tali società ad implementare l'Internal Control – Integrated Framework (1992).

Ancora più recentemente, basandosi sul COSO's Internal Control - Integrated Framework, è stato predisposto dal COSO il documento "Guidance on Monitoring Internal Control Systems" (January 2009) per supportare le aziende nel monitoraggio dei propri sistemi di controllo interno.

1.1.2.2COBIT® e IT Control Objectives for SOX

Per quanto riguarda la componente IT, la Legge 262/2005 non fornisce indicazioni puntuali sulle modalità con le quali effettuare la valutazione del sistema dei controlli in ambito IT. Inoltre, pur volendo far riferimento esclusivamente al modello COSO, questi risulta di non immediata applicazione per la componente IT.

Di conseguenza si pone il problema di individuare un framework di riferimento per i controlli IT la cui validità possa essere oggettivamente riconosciuta. In tal senso l'insieme di controlli definiti dalla metodologia COBIT® (Control Objectives for Information and related Technology, pubblicato dall'IT Governance Institute) si pone senza dubbio come un riferimento certo e di provata affidabilità.

COBIT® propone controlli di ampia portata che indirizzano obiettivi aziendali operativi e di conformità, ma non risultano strettamente collegati alla predisposizione dei documenti economico-finanziari, utilizzabili quindi per la conformità alla Legge 262/2005.

Per fornire quindi una risposta alla necessità di dettagliare maggiormente gli aspetti sul controllo IT rispetto allo schema proposto dal COSO, l'ITGI (IT Governance Institute) ha avviato un gruppo di lavoro avente l'obiettivo di emanare delle linee guida sulla tematica dei controlli IT, come parte integrante delle loro attività di valutazione della conformità alla normativa SOX (Sarbanes-Oxley Act, section 404 - luglio 2002 - US legislation).

Il primo risultato del gruppo di lavoro si è sostanziato nel documento "IT Control Objectives for Sarbanes Oxley", (aprile 2004)

Le attività sono proseguite anche successivamente, per raccogliere le esperienze che nel frattempo venivano dall'applicazione sul campo, fino alla pubblicazione del documento "IT Control Objectives for Sarbanes Oxley 2nd edition", (settembre 2006).

Il documento nella seconda edizione contiene perfezionamenti in merito a:

- maggiore focus sulle fasi di definizione del perimetro delle entità legali incluse nel progetto e dei relativi ambiti IT (espressione sinteticamente resa dalla prassi con il termine "scoping") e risk assessment
- prioritizzazione dei controlli
- gestione dell'elemento umano del cambiamento
- arricchimento delle linee guida sugli Application Controls
- approccio ai fogli di calcolo
- cross-reference con COBIT® 4.0
- perfezionamento delle linee guida sulla segregazione delle funzioni (segregation of duties)

Il documento fornisce le seguenti indicazioni sul sistema dei controlli IT:

- Roadmap per la compliance SOX: il capitolo fornisce indicazioni relativamente agli step progettuali da implementare per indirizzare la compliance SOX. Gli step suggeriti sono suddivisi in:

  - pianificazione e ambito dei controlli IT
  - valutazione del rischio IT
  - documentazione dei controlli
  - valutazione del disegno e dell'operatività dei controlli
  - individuazione, prioritizzazione e sistemazione delle "deficiencies" riscontrate
  - costruzione di un modello di gestione della compliance SOX

- Relazioni COSO/COBIT® e classificazione dei controlli IT: le appendici B, C, D e J descrivono in maniera dettagliata:

  - le relazioni tra i domini del COBIT® e i componenti del COSO e la mappatura puntuale tra i processi COBIT® (sia Entity che Activity Level) e i componenti COSO
  - gli Entity Level IT Controls (IT ELC), il cui obiettivo è quello di ottenere una comprensione della cultura e dello stile operativo dell'organizzazione
  - gli Activity Level controls, inclusi i processi di gestione dell'end user computing corredati di esemplificativi circa le modalità di effettuazione dei test; inoltre vengono identificati mediante il simbolo i controlli "più rilevanti"
  - gli Application Controls con esempi relativi ai principali processi di business e del financial reporting.

Il documento fornisce inoltre un insieme di strumenti utili come linea guida per un progetto di adeguamento alla SOX, quali un esempio di mappatura dell'architettura tecnologica, un tool per la stima di un progetto di compliance IT, tabelle di esempio per la valutazione del rischio e la rilevazione dei controlli ed infine degli elementi in merito alla segregazione delle funzioni nelle applicazioni afferenti il financial reporting.

1.1.3 Guide interpretative

A seguito dell'emanazione della normativa sul Dirigente Preposto, sono state pubblicate alcune guide interpretative.

A titolo di esempio si ricordano:
- maggio 2007: "Position Paper" dell'Associazione Nazionale Direttori Amministrativi e Finanziari (ANDAF)
- dicembre 2007: "Linee Guida per lo svolgimento delle attività del dirigente preposto" di Confindustria
- giugno 2008: "L'attività attestativa del "dirigente preposto" e degli organi amministrativi delegati alla luce dell'art. 154 bis TUF (D.LGS N. 58/1998)" Circolare ABI

Dai documenti citati si evince il ruolo centrale dell'Information Technology come componente fondamentale delle "adeguate" procedure amministrative e contabili.

Ampio rilievo viene attribuito sia agli aspetti generali relativi allo sviluppo e alla gestione dei sistemi informativi che supportano i processi (c.d. IT General Controls - ITGC), sia al tema dei controlli automatici a livello di singolo processo aziendale (c.d. Application Controls).
Viene ritenuto essenziale che queste tipologie di controllo siano considerate sia nella fase di rilevazione e analisi del disegno dei controlli che in quella di verifica dell'efficacia operativa e di valutazione delle carenze.

Più in particolare la circolare ABI indica che i modelli COSO e COBIT®"…*possono costituire un utile riferimento nello svolgimento delle attività operative..*". Tale indicazione viene rimarcata mediante l'inserimento nella "Bozza di modello di attestazione tipo" di una specifica clausola che descriva il modello di riferimento utilizzato per la valutazione del sistema dei controlli.

1.1.4 Conclusioni

Il quadro di riferimento illustrato evidenzia che la responsabilità del DP, nell'attestare l'adeguatezza e l'effettiva applicazione delle procedure amministrative e contabili, non può prescindere dalla valutazione del sistema informativo aziendale in cui le procedure stesse sono inserite.

L'affidabilità di tale attestazione si fonderà sull'esistenza di un adeguato sistema di regole del governo dell'infrastruttura tecnologica e degli applicativi, che può essere realizzato utilizzando le indicazioni del framework COBIT® così come specificamente adattato ai fini della compliance al Sarbanes Oxley Act.

In particolare la seconda edizione di tale documento consente, attraverso specifiche indicazioni metodologiche e di priorità dei controlli da implementare, di realizzare un modello di controllo adeguato alle diverse realtà aziendali che sia opportunamente bilanciato anche rispetto al trade-off tra costi e copertura dei rischi.

1.1.5 Fonti e riferimenti

Di seguito si fornisce una tabella riepilogativa delle fonti normative e dei riferimenti metodologici che possono essere utili ai fini di approfondimento della materia.

Fonte normativa nazionale:

- Legge 262/2005: L. 28 dicembre 2005, n. 262, modificata dal D. Lgs. 29-12-2006 n. 303

Fonte normativa internazionale:

- Sarbanes-Oxley Act del 2002 – luglio 2002
- J-SOX, Japan's Financial Instruments and Exchange Law, June 14th, 2006.

Guide interpretative:

- Position Paper ANDAF - Documento di consultazione
  "Il dirigente preposto alla redazione dei documenti contabili e societari"
  Analisi, interpretazioni e proposte
  ANDAF
  Maggio 2007 (Ver3.2)

- Linee Guida di Confindustria
  "Linee Guida per lo svolgimento delle attività del dirigente preposto alla redazione dei documenti contabili societari ai sensi dell'art 154-bis TUF"
  CONFINDUSTRIA - Area Strategica Fiscalità, Finanza e Diritto d'Impresa Nucleo Affari Legali, Finanza e Diritto d'Impresa – Gruppo di lavoro "Diritto Societario"
  13 dicembre 2007

- Circolare ABI
  "L'attività attestativa del "dirigente preposto" e degli organi amministrativi delegati alla luce dell'art. 154 bis TUF (D.LGS N. 58/1998)"
  Associazione Bancaria Italiana
  Circolare, Serie legale n.5
  30 maggio 2008

Riferimenti metodologici

- **COBIT® 4.1**
  IT Governance Institute, maggio 2007, di cui è disponibile la versione italiana curata da AIEA

- **IT Control Objectives for Sarbanes-Oxley**
  The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition
  IT Governance Institute, settembre 2006, di cui è disponibile la versione italiana curata da AIEA

- **Internal Control - Integrated Framework**
  By the Committee Of Sponsoring Organizations of the Treadway Commission (COSO) (1992)

- **Enterprise Risk Management – Integrated Framework**
  By the Committee Of Sponsoring Organizations of the Treadway Commission (COSO) (settembre 2004)

- **Guidance on Monitoring Internal Control Systems**
  By the Committee Of Sponsoring Organizations of the Treadway Commission (COSO) (January 2009)

- **Internal Control over Financial Reporting – Guidance for Smaller Public Companies** elaborata da PWC e pubblicata dal COSO (Committee Of Sponsoring Organizations of the Treadway Commission) nel giugno 2006 e sua traduzione in italiano a cura di AIIA e PWC maggio 2008.

- **PCAOB Audit Standard No. 2 - giugno 2004**

- **PCAOB Audit Standard No. 5 – luglio 2007**

- **"Management's report on internal control over financial reporting"** SEC dicembre 2006

- **GAIT Guide to the Assessment of IT General Controls Scope Based on Risk** The Institute of Internal Auditors gennaio 2007

1.2 Allegato – Dettaglio per fonte/riferimento

1.2.1 Position Paper ANDAF

Documento di consultazione
IL DIRIGENTE PREPOSTO (DP) ALLA REDAZIONE DEI DOCUMENTI CONTABILI E SOCIETARI

Analisi, interpretazioni e proposte - maggio 2007 (Ver3.2)

IL DP ED I SISTEMI INFORMATIVI AZIENDALI (pag 16)

Al fine di poter disporre di un sistema organizzativo, contabile e di controllo idoneo a consentire, oltre che un'efficiente gestione anche la prevenzione di comportamenti devianti rispetto alle policy aziendali e/o di illeciti nei casi più gravi, il DP deve poter fare affidamento sulla funzione sistemi informativi, che in larga misura governa i vari processi aziendali.
Sono da segnalare, con riferimento all'information technology due aspetti di particolare importanza per il DP:
(a) occorre considerare che le responsabilità affidate al DP, cui la legge chiede di attestare "l'adeguatezza e l'effettiva applicazione delle procedure …", non possono prescindere dalla valutazione del sistema informativo aziendale, in cui le procedure stesse sono inserite. L'analisi del corretto disegno delle procedure e quindi dei singoli processi che esse descrivono, dovrà inevitabilmente prendere in esame anche i processi informatici;
(b) il DP può e deve poter utilizzare gli strumenti informatici per lo svolgimento del suo lavoro e fare affidamento sulla notevole evoluzione che l'Information & Communication Technology (ICT) ha fatto registrare in questi ultimi anni in termini soprattutto di gestione integrata dei processi aziendali e di soluzioni di monitoraggio della compliance alle normative interne ed esterne.

PAG. 19
Inoltre il DP dovrà avere:
(a) (b) (c) (d) (e) [omissis]
(f) la partecipazione al disegno dei sistemi informativi che hanno impatto sulla situazione economica, patrimoniale e finanziaria;

Tra i "mezzi" dei quali si dovrà fare in modo che il DP possa poter disporre nell'adempimento dei compiti attribuitigli, si indicano i seguenti:
(a) (b) (c) [omissis]
(d) possibilità di utilizzo, ai fini del controllo, dei sistemi informativi.

IL DP E LA FUNZIONE SISTEMI INFORMATIVI (pag 54)

Al fine di poter disporre di un sistema organizzativo, contabile e di controllo, idoneo a consentire, oltre che un'efficiente gestione anche la prevenzione di comportamenti devianti rispetto alle policy aziendali e/o di illeciti nei casi più gravi, il DP deve poter fare affidamento sulla funzione sistemi informativi, che in larga misura governa i vari processi aziendali.
Sono da segnalare, con riferimento all'information technology, due aspetti di particolare importanza per il DP:
(a) occorre considerare che le responsabilità affidate al DP cui la legge chiede di attestare "…l'adeguatezza e l'effettiva applicazione delle procedure …" non possono prescindere dalla valutazione del sistema informativo aziendale in cui le procedure stesse sono inserite. L'analisi del corretto disegno delle procedure e quindi di singoli processi che esse descrivono dovrà inevitabilmente prendere in esame anche i processi informatici;

(b) il DP può e deve poter utilizzare gli strumenti informatici per lo svolgimento del suo lavoro e fare affidamento sulla notevole evoluzione che l'Information & Communication Technology (ICT) ha fatto registrare in questi ultimi anni in termini soprattutto di:

- gestione integrata dei processi aziendali;
- certificabilità del dato prodotto dai sistemi informativi;
- soluzioni di monitoraggio della compliance alle normative interne ed esterne.

La diffusione di sistemi informativi ERP (Enterprise Resource Planning) abilita una gestione strutturata ed integrata (da parte di tutte le unita organizzative) degli eventi aziendali, garantendo al tempo stesso la tracciabilità di ogni singolo step di processo: ciò rappresenta, con riferimento agli adempimenti contabili, un elemento imprescindibile per poter attuare i controlli circa la corretta applicazione di principi e procedure amministrative.

Attraverso un sistema ERP di gruppo sarà molto più agevole per il DP verificare che la raccolta delle informazioni provenienti dalle società incluse nell'area di consolidamento sia completa, effettuare controlli di conformità dei dati, accertare che siano state svolte correttamente le varie procedure di eliminazione delle operazioni intercompany, verificare le quadrature etc.

Va inoltre considerato che un sistema ERP consente anche di rendere meno praticabili comportamenti devianti rispetto alle procedure statuite, e consente di concentrare i controlli a monte ed a valle dei processi di elaborazione intermedi.

A completamento della rapida disamina circa le funzionalità informatiche che il DP dovrebbe riscontrare all'interno del proprio "sistema organizzativo, contabile e di controllo", occorre infine sottolineare l'estrema importanza ricoperta dalla gestione dei profili di accesso al sistema stesso, posto l'enorme aumento dei c.d. computer crime, con riferimento sia alla segregation of duties che al rispetto delle policy aziendali.

Il DP a tal fine, con il supporto dell'ente Information & Communication Technology (ICT) e della funzione internal auditing, dovrebbe:

- definire e delimitare a quali sistemi, moduli applicativi e transazioni l'utente può essere abilitato (profili autorizzativi);
- verificare i profili autorizzativi associati a ciascun utente o gruppo di utenti evidenziando eventuali anomalie nei profili (in modo da evitare preventivamente accessi non autorizzati);
- avere evidenza periodica degli utenti che hanno effettuato registrazioni contabili ed altri eventi di rilevanza amministrativa, con un corredo informativo in grado di riportare il tipo di transazione, data, ora, etc.;
- disporre di un set di reporting di controllo che contenga ex post eventuali anomalie nelle transazioni effettuate, con evidenza dell'utenza cui si riferisce e dell'anomalia riscontrata rispetto alle procedure aziendali in essere.

Il DP dovrebbe inoltre ricevere adeguate "rassicurazioni" dal responsabile dell'Information & Communication Technology, anche attraverso specifiche attestazioni, circa (i) il corretto funzionamento delle infrastrutture e delle applicazioni per l'acquisizione, elaborazione, trasmissione e rappresentazione delle informazioni amministrativo-contabili, cosi come previsto dal disegno funzionale, (ii) che eventuali "anomalie" o malfunzionamenti di natura tecnica siano tempestivamente individuati e risolti e (iii) l'esistenza di adeguate procedure volte a garantire la salvaguardia e conservazione del patrimonio informativo aziendale (procedure anti-intrusione/fire-wall), nonché il ripristino delle funzionalità del sistema in caso di guasti o incidenti (procedure di back-up/restore, disaster recovery, etc.).
La gestione dei profili di accesso ai sistemi informativi aziendali dovrà essere ancor più scrupolosa e stringente nel caso in cui i sistemi informativi siano, in tutto o in parte, oggetto di un servizio di outsourcing o nel caso in cui la manutenzione (ordinaria e straordinaria) ed i nuovi sviluppi siano seguiti nell'ambito di progetti informatici che prevedono l'erogazione di un supporto al responsabile dell'Information & Communication Technology, da parte di fornitori esterni.

Nota 34
Il ruolo che il DP deve necessariamente ricoprire, durante la fase di implementazione o review di un sistema esistente e da considerarsi assolutamente primario. Nel primo caso, il DP deve prendere parte attivamente alle attività di disegno, approvando la "blueprint" finale per poi appurare che la configurazione della soluzione applicativa sia del tutto coerente con i principi e le funzionalità precedentemente definite. Nel caso di review di una soluzione pre-esistente al suo insediamento, il DP dovrà valutare, sulla base dell'esito del risk assessment, la rispondenza delle procedure informatiche e, qualora necessario, richiederne lui stesso gli aggiornamenti ritenuti opportuni.

Nota 36
Uno dei problemi maggiori riscontrati nell'applicazione della SOX negli USA è stato "normalizzare" ed integrare molte elaborazioni critiche che venivano eseguite "fuori linea" con programmi di produttività individuale, quali fogli elettronici e data base stand alone.

LA VALUTAZIONE DEI RISCHI (pag 84)
Ogni società deve dotarsi di procedure per valutare tutti i rischi potenziali che possono minare il raggiungimento degli obiettivi aziendali (attività di risk assessment); in particolare la valutazione dei rischi deve essere condotta sia a livello societario complessivo (a livello di entità) sia a livello di specifico processo.

Nel primo ambito rientrano in particolare, con riferimento all'informativa finanziaria, i rischi di frode, che possono peraltro coinvolgere il management aziendale (management override), ed i rischi di non corretto funzionamento dei sistemi informatici. A livello di processo i rischi connessi all'informativa finanziaria (sottostima, sovrastima delle voci, non accuratezza dell'informativa, etc.) vanno analizzati a livello delle singole attività elementari che compongono i processi.

L'ATTIVITA' DI CONTROLLO (pag 84)
Il CoSO Report include una serie di attività di controllo che possono essere implementate in una organizzazione, tra le quali ci sono:

- controlli specifici a livello di processo, effettuati nello svolgimento delle attività operative e che hanno, quindi, l'obiettivo di prevenire, individuare o portare alla correzione di errori/irregolarità;
- controlli di tipo generale, che sono normalmente elementi strutturali del sistema di controllo, quali, ad esempio, la segregazione dei compiti tra loro incompatibili, i controlli generali sui sistemi informatici, etc.

(pag 89)
In generale è indubbio che l'adeguatezza del sistema informativo aziendale rappresenti un componente fondamentale delle "adeguate" procedure amministrative e contabili; in questo ambito assumono rilievo sia gli aspetti generali relativi allo sviluppo e gestione del sistema (c.d. general computer control) sia i controlli automatici previsti sulle diverse aree applicative a livello di singolo processo aziendale (c.d. application control).

1.2.2 Linee Guida di Confindustria

Linee Guida per lo svolgimento delle attività del dirigente preposto alla redazione dei documenti contabili societari ai sensi dell'art 154-bis TUF – 13 dicembre 2007
CONFINDUSTRIA- Area Strategica Fiscalità, Finanza e Diritto d'Impresa Nucleo Affari Legali, Finanza e Diritto d'Impresa – Gruppo di lavoro "Diritto Societario

Alla luce di quanto detto, il DP deve disporre dei poteri di [1]:
1. [omissis];
2. [omissis];
3. approvazione di tutte le procedure aziendali che hanno un impatto sulla situazione economica, patrimoniale e finanziaria, nonché partecipazione al disegno dei sistemi informativi. (parte I - §4.1 pag 16)

[1] Vedasi in particolare le parti sottolineate

Si evidenziano, di seguito, alcuni esempi di fattori di rischio potenziale, relativi ai processi transazionali e ai processi di valutazione e stima, suddivisi in base alle tre tipologie sopra indicate: *i. processi transazionali*

- tra le problematiche identificate nel passato:
- [omissis];
- tra i fattori di cambiamento:
  eventuale modifica o sostituzione dei sistemi informativi che comportano migrazioni massive di dati o riorganizzazione delle attività operative connesse, incluse le attività di controllo; (parte II - §3.2 pag 36)

Tra i controlli interni posti in essere per fronteggiare specifici rischi vi sono anche i controlli automatici (*application controls*).

Il processo di valutazione deve quindi prendere in considerazione il disegno e l'operatività dei controlli di sistema e dei controlli generali IT riferiti al perimetro di analisi. Si evidenzia che l'identificazione dei rischi e dei controlli relativi ai sistemi informativi non deve essere considerata un processo separato bensì parte integrante dell'intero approccio di valutazione del sistema di controllo sul Financial Reporting. (parte II - §3.2 pag 37)

Tali attività (*la rilevazione e analisi del disegno dei controlli e la verifica dell'operatività dei controlli*) dovranno essere svolte per tutti i controlli ritenuti rilevanti per l'attendibilità del Financial Reporting. In particolare, ne è richiesto lo svolgimento per i controlli appartenenti:
• al processo di chiusura contabile/Financial Reporting (*closing the book*) 32;
• ai processi/rischi risultati rilevanti in base all'individuazione delle aree oggetto di attività;
• al processo dei controlli generali informatici relativamente ai sistemi informativi che supportano i processi. (parte II - §4.2 pag 41)

Avendo individuato i sistemi che supportano i processi a rischio e i controlli inclusi in tali processi, dovranno essere verificati anche i controlli che riguardano i sistemi informativi (parte II - §4.4 pag 44)

Le carenze riguardanti i controlli generali sui sistemi informativi dovranno essere considerate e valutate insieme alle carenze rilevate nei controlli applicativi. (parte II - §5 pag 44)

1.2.3 Circolare ABI Serie legale n.5 del 30 maggio 2008

Il modello di riferimento

1. Al fine di poter adempiere agli oneri attestativi di cui all'art.154 bis, comma 5, TUF il dirigente preposto dovrà definire un modello di governo amministrativo finanziario, funzionale a garantire e verificare in via continuativa l'adeguatezza e l'effettiva applicazione delle procedure amministrative e contabili (anche a livello di gruppo).

La normativa italiana non fa riferimento a specifici standard per la valutazione dell'efficacia dei processi e dei controlli; a tale proposito si ricorda che organismi internazionali hanno pubblicato modelli che risultano largamente utilizzati a livello internazionale (quali ad esempio il COSO Framework e, per la componente IT, il COBIT® Framework), che pertanto possono costituire un utile riferimento nello svolgimento delle attività operative.

[omissis]

Attestazione del bilancio consolidato ai sensi dell'art.81 – ter del Regolamento Consob n. 11971 del 14 maggio 1999 e successive modifiche e integrazioni

1. I sottoscritti……in qualità di Amministratore Delegato,……, in qualità di Dirigente preposto alla redazione dei documenti contabili societari di…..attestano, tenuto anche conto di quanto previsto dall'art. 154-bis, commi 3 e 4, del decreto legislativo 24 febbraio 1998, n.58:

l'adeguatezza in relazione alle caratteristiche dell'impresa e
l'effettiva applicazione,

delle procedure amministrative e contabili per la formazione del bilancio consolidato nel corso dell'esercizio 2007.

2.1. (Il modello di riferimento)
La valutazione dell'adeguatezza delle procedure amministrative e contabili per la formazione del bilancio consolidato al 31 dicembre 2007 si e' basata su di un Modello definito da XYZ Spa in coerenza con il framework…(es Internal Control – Integrated Framework emesso dal Committee of Sponsoring Organizations of the Treadway Commissione e il framework COBIT®, per la componente dei sistemi IT, che rappresentano standard di riferimento per il sistema di controllo interno generalmente accettati a livello internazionale).

[omissis]

1.2.4 Internal Control - Integrated Framework By the Committee Of Sponsoring Organizations of the Treadway Commission (1992)

Il COSO Framework definisce il controllo interno come un processo che si prefigge di fornire una ragionevole garanzia della realizzazione degli obiettivi rientranti nelle seguenti tre categorie:

- efficacia ed efficienza delle attività operative (Operations);
- attendibilità dell'informativa finanziaria (Financial Reporting);
- conformità alle leggi e ai regolamenti in vigore (Compliance).

Il COSO Framework è caratterizzato da cinque componenti che riguardano:

1) **Ambiente di Controllo**: rappresenta l'ambiente (elemento della cultura aziendale) che determina il livello di "sensibilità" del personale alla necessità di controllo e include i seguenti elementi:
   - filosofia e stile gestionale del Management;
   - integrità, valori etici e competenza del personale;
   - modalità di delega, organizzazione e sviluppo professionale;
   - capacità di indirizzo e guida dell'alta direzione;
2) **Valutazione del Rischio**: consiste nell'individuazione e analisi dei fattori che possono pregiudicare il raggiungimento degli obiettivi aziendali e determina le modalità di gestione dei rischi sulla base dei seguenti elementi:
   - ambiente micro e macro economico;
   - situazione normativa;
   - condizioni operative aziendali;
3) **Attività di Controllo**: costituisce l'insieme delle politiche e delle procedure che assicurano la corretta applicazione delle direttive del Management e si traduce in:
   - approvazioni e autorizzazioni;
   - verifiche;
   - esami della performance;
   - protezione dei beni aziendali;
   - separazione dei compiti.
4) **Informazione e Comunicazione:** rappresenta il principio in base al quale le informazioni pertinenti devono essere individuate e diffuse nei modi e nei tempi appropriati per consentire alle persone di assolvere le proprie responsabilità. Il Management deve comunicare in modo chiaro a tutto il personale l'importanza che assumono le singole attività aziendali sul sistema di controllo interno. Si tratta di una componente "trasversale" alle altre componenti del controllo interno.
5) **Monitoraggio**: consiste nel monitoraggio del Sistema di Controllo Interno, al fine di valutare nel tempo la qualità della sua performance attraverso attività di supervisione continua e/o valutazioni periodiche.

Di seguito sono riportate le principali componenti che fanno riferimento all'Information Technology.

La **componente "Attività di Controllo"** viene descritta attraverso differenti tipologie di controllo (preventivi, a posteriori, manuali e di sistema) comunemente utilizzate tra cui viene citata la componente ICT.

Nell'ambito della stessa componente ("Attività di Controllo"), il Framework sottolinea la rilevanza dei controlli sui Sistemi Informativi della società al fine del raggiungimento degli obiettivi di affidabilità del Reporting e conformità a leggi e regolamenti. Definisce così due tipologie di controlli ICT, **Generali ed Applicativi.**

La **componente "Informazione e Comunicazione**" sottolinea i principi di riservatezza, integrità e disponibilità delle informazioni conservate e prodotte dai Sistemi Informativi.

Un ulteriore contributo si trova nella **componente "Ruoli e Responsabilità**" e fa riferimento ai Service Provider per sottolineare che la responsabilità del management si estende anche alle attività affidate a terzi.

1.2.5 Internal Control over Financial Reporting – Guidance for Smaller Public Companies By the Committee Of Sponsoring Organizations of the Treadway Commission

Traduzione in italiano a cura di Institute of Internal Audit e Price Waterhouse and Coopers (maggio 2008).

Di seguito sono riportati i principali paragrafi utili per lo svolgimento delle attività di ricerca.
L'Executive summary, destinato ai componenti il consiglio di amministrazione e ai senior manager (paragrafo Tecnologie Informatiche pag. 8), suggerisce quale soluzione per superare possibili carenza di risorse IT, la scelta di software sviluppati esternamente e con manutenzione esternalizzata.

La seconda parte della Guida descrive per tali imprese le peculiarità e come esse possano influenzare il controllo interno; sono così illustrati 20 principi, desunti dal COSO Framework, con indicazioni circa la loro applicabilità pratica.
I paragrafi Information Technology e Controlli Automatizzati (pag. 31,32) oltre a ribadire l'utilità dei software sviluppati e gestiti esternamente, si focalizzano sui controlli automatizzati che possono migliorare l'affidabilità dei risultati operativi, automatizzare le riconciliazioni, facilitare il reporting delle anomalie ed agevolare la Separazione dei Compiti.

Il Principio n°14 della componente "Attività di Controllo" (da pag. 101 a pag. 112) è specifico per l'Information Technology e prende in considerazione sia i controlli applicativi, sia i controlli generali sui sistemi informativi. Sono quindi riportate n°6 categorie per i controlli IT (sviluppo sistemi, cambiamenti di sistema, sicurezza accessi, etc.).

I Principi n°15 e n°16 della componente "Informazioni e Comunicazione" (da pag. 114 a pag. 118) considerano la completezza, l'accuratezza e la tempestività dei dati provenienti dai sistemi informativi quali elementi fondamentali per consentire il conseguimento degli obiettivi del financial reporting.

2 PERIMETRO DI INDAGINI E RISK BASED APPROACH

(FOCUS GROUP 2)

2.1 Individuazione del perimetro di applicazione (Scoping)

2.1.1 Premessa

Il processo di definizione del perimetro IT di applicazione ai fini del raggiungimento della conformità espressa nel Legge 262/2005, consiste nell'individuazione degli elementi che dovranno avere controlli che si qualificano in termini di adeguatezza di disegno ed effettiva operatività e per la capacità di garantire la qualità e l'affidabilità della reportistica finanziaria.

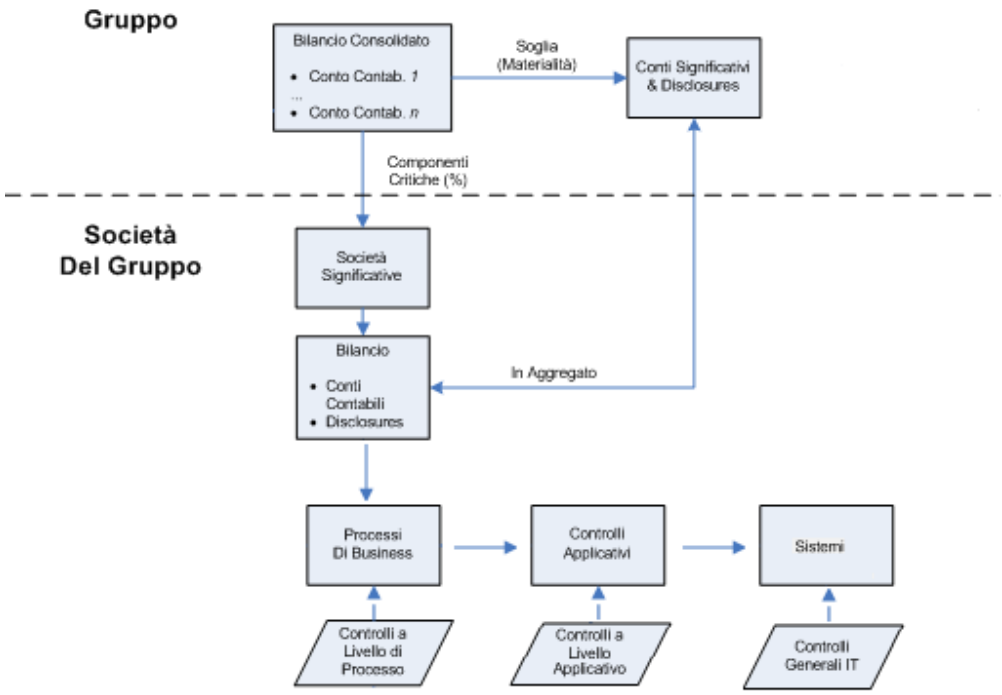
Il presente paragrafo illustra gli aspetti da considerare al fine di individuare il perimetro di applicazione dei controlli generali IT che consistono in:

- Processi IT: intesi come le macro-attività della funzione IT;
- Obiettivi di controllo: gli obiettivi di controllo necessari a garantire la corretta operatività dei processi IT;
- *Applicazioni*: l'insieme dei software gestionali utilizzati nell'ambito dei processi amministrativo-finanziari che concorrono alla gestione dei flussi transazionali e alla formazione della reportistica finanziaria;
- *Software di base, Hardware e Networking* associati alle applicazioni al punto precedente.

In maggiore dettaglio l'insieme dei processi IT e degli obiettivi di controllo sono individuabili quale conseguenza della scelta del Framework dei controlli, mentre le applicazioni software e la sottostante componente tecnologica sono individuate dal processo descritto nei paragrafi a seguire.

Processo di individuazione del perimetro di applicazione dei controlli generali IT

Le fasi logiche di individuazione del perimetro di applicazione dei controlli generali IT derivano dalle modalità più generali di definizione del perimetro di applicazione e di valutazione dei controlli ai fini della Legge 262/2005.
Nello schema a seguire è rappresentato in maniera semplificata un modello di identificazione del perimetro (o "scoping") di applicazione basato su elementi quantitativi a partire dai valori economici e patrimoniali di un gruppo societario.



Oltre agli elementi quantitativi si dovranno considerare altre valutazioni di rischiosità che possono essere già presenti in società, ancorchè non esprimibili in quantità monetarie che sono definibili come elementi qualitativi.

Definizione del perimetro – Elementi quantitativi

La fase di definizione del perimetro in funzione di elementi qualitativi parte dall'identificazione dei conti contabili significativi e delle disclosure e questo a fronte del complessivo processo di "Scoping".

Individuati i conti di bilancio e le disclosure in perimetro si identificano le applicazioni a supporto del processo o che forniscono i dati di business che partecipano alla formazione del conto/disclosure.

Per tale attività è sempre utile definire la mappatura applicativa di riferimento (c.d. Application Matrix) che andrà a contenere perlomeno le informazioni di:

- Processo di business di riferimento
- Sotto-processo di business di riferimento
- Nome dell'applicazione
- Operating & Network systems
- Piattaforma IT di riferimenti (OS, DB, Linguaggio di programmazione, etc)
- Referente applicativo IT
- Modalità di implementazione (Acquistato, personalizzato, sviluppato in house, ecc…)

Quale ultimo passaggio, a conferma o meno delle applicazioni in perimetro, si dovrà effettuare un confronto tra i controlli applicativi in perimetro per i processi di Business, con le applicazioni individuate. Tale verifica permetterà di confermare la correttezza e completezza del parco applicativo interessato dai processi di conformità ai fini della Legge 262/2005.

Definizione del perimetro – Elementi qualitativi
Come accennato possono concorrere alla riduzione od ampliamento del perimetro di valutazione dei controlli generali IT altri aspetti non direttamente collegabili ad elementi a valori patrimoniali o economici dell'azienda. E' suggerita la valutazione ed applicazione degli elementi qualitativi successivamente a quelli quantitativi.

Tra gli elementi qualitativi si dovranno considerare aspetti quali:

- "Vicinanza" degli "oggetti" informatici alle informazioni più rappresentative della reportistica finanziaria (ad es. l'applicazione che permette il consolidamento del bilancio è più rilevante ai fini della Legge 262/2005 rispetto a quella che supporta il processo di rilevazione delle presenze). Tale caratteristica inoltre concorre alla definizione di rilevanze decrescenti a seconda che si tratti dell'applicazione e dei suoi dati, del sistema operativo e del software di base, del networking.
- Volume delle attività, complessità, ed omogeneità delle transazioni;
- Peculiarità e specificità del processo di business supportato dall'applicazione (ad esempio la dipendenza da dati esterni per la preparazione della nota informativa del bilancio);
- Ulteriori fattori di rischio individuati attraverso altri processi o funzioni aziendali (ad es. Enterprise Risk Management, Internal Audit, External Audit, ecc…);
- Storia degli errori in relazione alle applicazioni;
- Presenza di terze parti;
- Cambiamenti significativi occorsi (ad es. acquisizioni, cambi di sistema, ecc.).

Presenza di Service Provider
In presenza di processi IT esternalizzati, i relativi controlli andranno inclusi nel perimetro nel caso in cui siano individuati quali "rilevanti" dal processo di valutazione "quantitativo" e "qualitativo".
In sostanza la trattazione in termini di "scoping" dei controlli esternalizzati segue il medesimo approccio di quelli presenti in società.

Ambienti di elaborazione e loro individuazione
Individuate le applicazioni software in perimetro sarà necessario individuare gli "ambienti elaborativi" o "layer" ("piattaforme") di interesse identificandone le caratteristiche comuni in termini di caratteristiche del controllo quali la frequenza, la tipologia, l'organizzazione preposta.

Tale processo si renderà necessario al fine di minimizzare la documentazione necessaria per descrivere il sistema di controllo interno, oltre che gli impegni necessari per le verifiche di operatività. In questo modo, infatti, i controlli effettuati su un certo "ambiente operativo" o "layer" garantiscono la copertura dei rischi per tutte le applicazioni ivi ricomprese.

2.2 Adozione di un Risk Based Approach

La ragionevole assicurazione di un corretto trattamento dell'informazione contabile (integrità, completezza), l'affidabilità dei controlli applicativi e delle procedure automatiche che consentono la produzione della reportistica finanziaria, dipendono dalla qualità dei controlli generali sull'IT.

Considerata la loro natura pervasiva (trasversali alle applicazioni), gli IT General Controls devono essere sistematicamente e periodicamente testati per garantire la loro efficacia ed efficienza e per verificare il completamento di eventuali azioni correttive in un adeguato arco temporale, al fine di minimizzare i controlli sulle procedure automatiche finanziariamente critiche.

Questo condurrebbe ad un'analisi dell'operatività di tutti i controlli interni a presidio delle funzionalità di Information Technology, inclusi quindi anche quei controlli interni che non hanno un impatto diretto sull'informativa finanziaria. Tale accezione permette di ottenere un elevato livello di efficacia, ma appare opportuno, per motivi di efficienza[2], restringere il perimetro di analisi degli IT General Controls in funzione dei rischi intrinseci alle funzionalità IT e del loro impatto dal punto di vista finanziario.

Ciascuno dei processi/controlli tendenzialmente opera sulle quattro piattaforme (layer) ITGC generalmente riconosciute (applicativa, database, sistema operativo e infrastruttura di rete).
Il rischio per l'affidabilità dell'informativa contabile e di bilancio può essere valutato e indirizzato contemporaneamente per ciascuno di questi quattro layer (es. il monitoraggio degli accessi) tenendo tuttavia in considerazione che i rischi individuabili in ciascun layer hanno un impatto differente sull'integrità dell'informativa contabile e di bilancio (nota 2)[3].

[2] Il bilanciamento tra estensione delle verifiche di efficacia e limitazione del perimetro per ragione di efficienza può essere utilmente basato sull'analisi dei rischi e sul fattore tempo. L'efficacia cresce al nascere dei controlli e relative verifiche, purché gli uni e le altre si concludano entro le scadenze programmate di monitoraggio del processo di business oggetto di controllo. Affinché il tempo dedicato al controllo sia sufficiente l'ordine di priorità dei rischi da monitorare fornisce l'elenco delle attività di processo che devono (alti rischi) o possono (medi rischi) essere monitorate.

[3] Generalmente i rischi relativi alla piattaforma applicativa e quelli inerenti la piattaforma dati hanno un impatto diretto sull'integrità dell'informativa contabile e di bilancio.

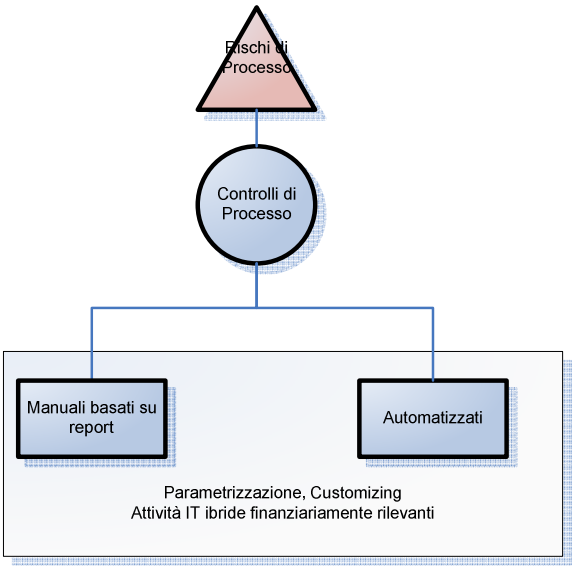
Il processo che può essere utile seguire per l'assessment dei rischi IT a fini della Legge 262/2005 è il seguente:

1. Identificare i processi "critici ai fini contabili" dell'IT, ovvero tutti quelli correlati ad obiettivi di controllo rilevanti per la produzione dell'informativa contabile;
2. Identificare i layer IT critici correlati alle applicazioni rilevanti;
3. Identificare i controlli a presidio dei rischi sottesi agli obiettivi di controllo;
4. Identificare i controlli chiave da sottoporre a testing in funzione della combinazione dei punti precedentemente citati.

Fase 1:
Per censire una lista di processi contabili critici, il focus deve essere posto sulle attività operative o di controllo effettuate da un individuo con il supporto di uno strumento (per esempio un report di sistema) e sui controlli automatizzati previsti all'interno delle quotidiane attività gestionali.

Dovranno essere considerati:

- Controlli automatizzati considerati contabilmente rilevanti.
- Report o altri controlli ibridi contabilmente rilevanti (controlli manuali effettuati dalla funzione IT, schermate, parametri,etc.)
- Cambiamenti ai dati che possono impattare sui controlli/report contabilmente rilevanti; pur non comportando modifiche alle logiche applicative, potrebbero causare errori nell'informativa contabile.(es. prezzi,limiti di credito, etc.).



E' da considerare inoltre l'eventuale presenza di funzionalità di sistema a supporto di quanto esposto ai punti precedenti che, se non appropriatamente considerate nella valutazione del rischio, e quindi non opportunamente monitorate, potrebbero causare, in situazioni di mancata/inappropriata operatività, errori materiali sulle componenti finanziarie correlate, non intercettate da alcun controllo.

La determinazione di quali ITGC sono importanti in riferimento all'impatto sull'informativa finanziaria è una fase altamente variabile a seconda del contesto di riferimento.
Verosimilmente gli ITGC più rilevanti a tal fine saranno quelli relativi alla:

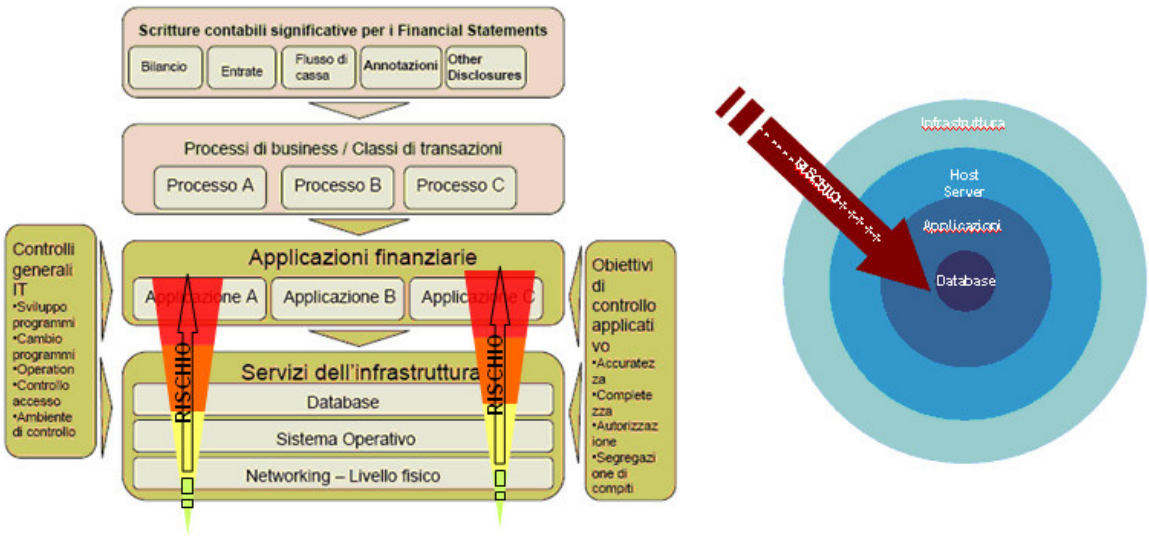
- Limitazione dell'accesso a programmi e dati, ovvero quei controlli a livello applicativo e DB che salvaguardano e regolano l'accesso dei diversi utenti a dati e programmi sensibili per la reportistica finanziare
- Verifica che le modifiche applicative siano autorizzate, correttamente definite, testate e adeguatamente implementate al fine di assicurare l'appropriatezza e la coerenza di funzionamento dei controlli applicativi (automatici e manuali basati su report)
- Operatività dei Sistemi Applicativi, enfatizzando quei controlli che impattano in maniera significativa sul flusso delle transazioni contabili (es. controlli di interfaccia e ripresa scarti).

Fase 2:

L'assessment del rischio inerente delle applicazioni e delle relative infrastrutture IT (database, sistemi operativi, network ed ambienti fisici) è necessario per determinare la natura e l'estensione dei controlli necessari per mitigare i rischi. È anche necessario comprendere il rischio inerente delle applicazioni e dei relativi sottosistemi per pianificare in modo appropriato il testing dell'efficacia operativa di tali controlli.

Nello sviluppare l'assessment del rischio inerente occorre riflettere sul numero dei fattori di rischio; prendendo in considerazione i fattori di rischio più comuni è possibile pervenire ad una prima base per un'analisi dei rischi plausibile e realistica.

Quanto più ci si avvicina alla possibilità di accedere in maniera diretta ai dati per la modifica, inserimento o cancellazione, tanto più si rischia di compromettere l'integrità, la completezza e l'efficacia dei controlli applicativi e delle procedure automatiche che concorrono alla produzione dell'informativa finanziaria. Il rischio è pertanto inversamente proporzionale alla distanza del layer preso in considerazione dai dati rilevanti ai fini dell'informativa finanziaria.



Fase 3

Determinati i processi critici secondo i criteri identificati con la fase 1 (es. manutenzione applicativa, accesso ai programmi e ai dati, operatività dei sistemi) e individuati i layer rilevanti in base a quanto dichiarato all'interno della fase 2 (es, Database, Parametrizzazione e codice sorgente dell'applicazione), occorre assegnare un grado di rischio alla combinazione processo/layer.

Domini		Technology Layer				
Processi	Controlli	Applicazione	Database	Sistema Operativo	Networking	Livello Fisico
Gestione e sviluppo dei programmi	Acquisizione e sviluppo del software	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Acquisizione delle infrastrutture tecnologiche	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Redazione e aggiornamento di politiche e procedure	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Gestione delle modifiche	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
Accesso ai programmi e ai dati e procedure di sistema	Definizione e gestione dei livelli di servizio	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Gestione dei servizi delle terze parti	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Assicurare la sicurezza dei sistemi	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Gestione della configurazione	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Gestione dei problemi e degli incidenti	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Gestione dei dati	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low
	Gestione delle procedure di sistema	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low	High/Medium/Low

Di solito, nel risk assessment, per determinare la probabilità e l'impatto che una minaccia si verifichi, si prendono in considerazione i fattori di seguito elencati:

1. **probabilità** che il rischio si verifichi;
2. potenziale **impatto** associato.

La probabilità che il rischio si verifichi è influenzata da:

- tipo di tecnologia in uso (complessa o semplice);
- aggiornamento della tecnologia in uso (anzianità dei supporti utilizzati e mole di modifiche subite in un anno);
- caratteristiche del personale (adeguato livello di risorse e competenze dello staff a presidio del supporto);
- natura dei processi (centralizzati o decentralizzati);
- esperienze ed avvenimenti passati;
- numerosità/frequenza di interventi di gestione emergenza
- grado di modifica, configurazione e personalizzazione del supporto
- esperienze ed avvenimenti passati.

Di seguito un esemplificativo:

Esempi di fattori di rischio	Probabilità maggiore del rischio	Probabilità minore del rischio
Complessità della tecnologia	Complessità, unicità, customizzazione, sviluppo *in-house*	Semplice, usato comunemente, nessuna customizzazione, pacchetto comprato in negozio (*off-the-shelf*)
Competenza/esperienza del personale	Risorse inesperte, mancanza di *training*, numero troppo limitato di persone, *turnover* alto	Risorse con esperienza, formate, specializzate in numero sufficiente, *turnover* basso
Localizzazione del processo	Decentralizzazione, multi locazione, *ad hoc*	Centralizzato, formalizzato, coerente
Esperienze passate	Storia dei problemi, compresi gli errori nel processing, criticità (*outages*) nei sistemi, corruzione dei dati	Nessun problema in precedenza

L'impatto potenziale considera che una debolezza nel processo/layer identificato potrebbe impattare l'efficacia di una o più funzionalità finanziariamente critiche del sistema, e quindi l'integrità dei controlli applicativi e delle procedure automatiche che consentono la produzione della reportistica finanziaria

Di seguito un esemplificativo per quanto riguarda la gestione dei cambiamenti e uno riguardante l'accesso a programmi, dati e procedure di sistema:
(NDR - Toffanin[i])

Layer	Gestione e Sviluppo dei programmi		
	Processo Critico?	Potenziali Obiettivi di Controllo Associati	Risk Rating
Application	**SI** L'applicazione contiene numerosi controlli automatici e altre funzionalità critiche, inclusi report di sistema e formule di calcolo. Il fallimento del processo di manutenzione applicativa a livello di modifica del codice sorgente potrebbe compromettere significativamente l'operatività dei controlli finanziariamente rilevanti.	• L'azienda usa una metodologia per l'intero ciclo di vista di sviluppo del software che comprende i requisiti per la sicurezza e l'integrità del processing. • La metodologia SDLC esplicita i requisiti necessari ed i controlli applicativi nel processing delle transazioni affinché quest'ultimo sia completo, accurato, autorizzato e valido. • L'azienda acquisisce/sviluppa sistemi software applicativi in accordo con tali processi di acquisizione, sviluppo e pianificazione.	**HIGH** - Numerosità interventi annui - Funzione AM sottostaffata
Database	**SI** La gestione, manutenzione e sviluppo del database relazionale sottostante l'applicazione sono stati considerati critici in quanto potrebbero inficiare l'integrità della struttura dati e dei dati stessi sensibili per le attività di business.	• La conversione dei dati è testata all'origine e alla destinazione per confermare che i dati sono completi, accurati e validi. • Sono posti in essere controlli per limitare la migrazione dei programmi in produzione alle sole persone autorizzate.	**LOW** - Il data dictionary non ha subito modifiche durante l'anno - Nessuna problematica riscontrata in passato
Operating System	**NO** I cambiamenti al SO (incluse le patch in emergenza) non sono stati considerati critici poiché modifiche inappropriate e/o effettuate senza una sufficiente attività di testing preventiva verrebbero individuate immediatamente in quanto la funzionalità applicativa ne risentirebbe immediatamente.		
Network	**NO** I cambiamenti all'architettura di rete non sono stati considerati critici in quanto la manutenzione di tutti gli elementi che costituiscono l'infrastruttura di rete dell'organizzazione (locali, apparati attivi, VPN IP, ecc.) è stata effettuata per garantire il tempestivo ripristino delle funzionalità del servizio di rete e/o apparati TLC, e non ha quindi impatto sulla funzionalità di processi finanziariamente rilevanti.		

Layer	Accesso ai programmi e ai dati e procedure di sistema		
	Processo Critico?	Potenziali Obiettivi di Controllo Associati	Risk Rating
Application	**SI** La gestione degli accessi all'applicazione è ritenuta rilevante in quanto vi sono controlli automatici che garantiscono l'accesso ristretto a determinate transazioni solo a determinati individui e funzioni	• Esiste una politica di sicurezza ed essa è stata approvata dall'appropriato livello dell'executive management; • Esiste ed è seguito un processo di controllo per effettuare periodicamente una review e confermare i diritti di accesso; • Esistono e sono osservate procedure per mantenere nel tempo efficaci meccanismi di autenticazione e di accesso ai sistemi IT; • Esistono e sono osservate procedure in relazione ad azioni tempestive da compiere per richiedere, stabilire, fornire, sospendere e chiudere gli account utente.	**HIGH** - Numerosità utenti a sistema - Dispersione territoriale filiali
Database	**SI** La gestione degli accessi al database relazionale sottostante l'applicazione è stata considerata critica in quanto potrebbe inficiare l'integrità dei dati sensibili per le attività di business.		**LOW** La gestione degli oggetti di database, lo sviluppo e il debug di codice PL/SQL e la creazione, l'esecuzione e l'ottimizzazione delle query SQL è gestita da un solo utente
Operating System	**NO** Gli accessi al SO non sono stati considerati critici in quanto eventuali modifiche non autorizzate non avrebbero impatto sulla integrità e funzionalità dei processi finanziariamente rilevanti.		
Networking	**SI** La gestione degli accessi alla componenti della rete aziendale da quella esterna è ritenuta rilevante in quanto vi sono dispositivi che garantiscono sia l'accesso esclusivo al personale autorizzato che un filtraggio dei dati in entrata/in uscita.	• Esiste ed è seguito un processo di controllo per effettuare periodicamente una review e confermare i diritti di accesso; • Esistono e sono osservate procedure di aggiornamento dei dispositivi di filtraggio/controllo dati; • Esistono e sono osservate procedure per mantenere nel tempo efficaci meccanismi di autenticazione e di accesso ai sistemi IT.	**HIGH** - Topologia di rete articolata e complessa - Elevata frequenza delle attività di aggiornamento dispositivi di filtraggio/controllo dati

Indipendentemente dai risultati, la documentazione delle decisioni effettuate e le motivazioni di tali scelte devono essere logiche e ricostruibili dal management / entità terze esterne. Un esempio didattico e non esaustivo potrebbe essere il seguente:

Dopo che è stato effettuato il risk assessment, il team sui controlli IT può considerare di analizzare nuovamente l'ambito del progetto ed eventualmente aggiornare le applicazioni ed i relativi sottosistemi presi in considerazione. In ogni caso il processo di risk assessment e le relative conclusioni devono essere chiaramente documentati. Ciò vale in particolare, quando qualche sistema è stato escluso dall'ambito del progetto. Se ci sono variazioni di ambito, deve essere aggiornato anche il piano di progetto; così come se si sono estesi o ridotti i test in seguito all'analisi dei rischi.

2.3 Collegamenti ad altri modelli aziendali di Governance eRisk Management

Il presidio della corretta produzione dell'informativa finanziaria o, in senso lato, l'insieme delle attività che un'azienda pone in essere in ottemperanza alla Legge 262/2005, si pongono in relazione con altre attività il cui fine è garantire la conformità al complesso normativo che regola il contesto di riferimento, nonché, più in generale, con gli strumenti di Governance che l'organizzazione pone in atto.

Senza la pretesa di esaurire l'argomento, di seguito alcuni ambiti normativi che richiedono di porre in atto specifiche procedure, organizzazioni e controlli:

- Nuovo Accordo di Basilea (cd Basilea 2)[4];
- D. Lgs. 231/2001 (Disciplina della Responsabilità Amministrativa) e reati informatici e successive modifiche ed integrazioni;
- Disposizioni di Vigilanza per la Continuità Operativa in casi di emergenza;

[4] Basilea 2, forma breve con cui ci si riferisce al **Nuovo Accordo sul Capitale sottoscritto dal Comitato di Basilea**, che ha rimpiazzato il precedente accordo noto come **Basilea 1**. Tale accordo, maturato nell'ambito del *Comitato di Basilea per la Supervisione Bancaria*, ha portato alla stesura di un documento condiviso, nel quale si introduce il concetto di requisito patrimoniale "risk based". Si sancisce che i requisiti patrimoniali delle banche devono essere commisurati all'effettivo ammontare di rischio assunto dalle stesse. I requisiti patrimoniali minimi che le banche sono tenute a rispettare costituiscono il **Primo pilastro** dell'accordo di Basilea. I rischi fondamentali per cui è necessario determinare il requisito patrimoniale sono di tre tipi: rischio di credito, rischio di mercato e rischio operativo.

Con riferimento al Nuovo Accordo di Basilea, si usa parlare di tre *pilastri*. Il primo, come definito da Basilea 1. Il **Secondo Pilastro** invece introduce la necessità della revisione prudenziale del requisito patrimoniale. Tale obbligo coinvolge sia gli istituti di vigilanza (per l'Italia la Banca di Italia), che devono sorvegliare sul rispetto degli obblighi patrimoniali, sia le stesse banche vigilate, che devono periodicamente autovalutare la propria esposizione complessiva ai rischi. Il **Terzo Pilastro** infine sancisce l'obbligo dell'informativa al pubblico per i soggetti sottoposti a vigilanza (le banche in primis).

Il **Comitato di Basilea** per la vigilanza bancaria è un organizzazione internazionale istituita dai governatori delle Banche centrali dei dieci paesi industrializzati (G10) alla fine del 1974, che opera sotto il patrocinio della Banca per i Regolamenti Internazionali (Bank for International Settlements: BIS), che ha sede a Basilea.

- D. Lgs. 196/03 (“Privacy”) e successive modifiche e integrazioni.

Per quanto poi attiene più genericamente ai presidi di Governance se non specifici in ambito Information Technology risultano di interesse:

- i modelli di Enterprise Risk Management;
- i sistemi e le procedure di Internal Auditing;
- i sistemi e le procedure di compliance interni;
- i sistemi di monitoraggio dei Livelli di Servizio;
- i sistemi di Incident Management;
- il monitoraggio fornitori per i servizi acquisiti dall’esterno;
- i modelli di pianificazione strategica e budgeting;
- i sistemi di controllo di gestione e di misurazione delle performance (Value Based Management - VBM, Economic Value Added – EVA^{TM}, ...);
- i sistemi di tariffazione interna nelle strutture di Gruppo con presidi di Governance/Operations accentrati.

Di norma, i controlli che attengono alle singole discipline, sono eseguiti in modo indipendente rispetto a quelli previsti da altri modelli, data la specificità di ciascun ambito. In ogni caso, i risultati delle attività di controllo possono risultare utili i altri contesti: per esempio le attività di controllo poste in atto per la Continuità operativa sono certamente di interesse in un ambito specifico quale quello della stima dei Rischi Operativi o di Credito.

La coesistenza di diversi modelli di governo pone all’attenzione del management l’opportunità di individuare punti di sinergia, nonché la necessità di assicurare la coerenza tra gli stessi modelli al fine di prevenire esiti discordanti o di dubbia interpretazione.

E’ verosimile che le principali sinergie siano identificabili nella messa a fattor comune di controlli integrati che dovrebbero caratterizzarsi per:

- esistenza di una tassonomia univoca dei processi aziendali;
- identificazione per i processi aziendali di diversi profili di sensibilità alle norme / procedure di controllo;
- effettuazione periodica di attività integrate di Risk and Control Assessment al fine di valutare esistenza, efficacia ed efficienza dei presidi di controllo;
- effettuazione periodica di test di effettività per verificare la corretta e continuativa messa in atto delle attività di controllo previste;
- produzione di reportistica periodica coordinata sugli esiti dei controlli inerenti i diversi modelli di Governo;
- analisi di coerenza della reportistica da parte degli organi preposti.

Tali momenti di sinergia possono risultare favoriti dalla predisposizione di cruscotti aziendali di sintesi che permettano di raccogliere e monitorare le eventuali azioni correttive ed identificarne le priorità di realizzazione.

3 CONTROLLI GENERALI IT

(FOCUS GROUP 3)

3.1 ***Entity Level Controls***

Il concetto di Entity Level Controls (ELC) è legato a quelle attività di verifica relative a processi, sistemi e procedure messe in atto da una azienda in modo da mitigare il rischio di errori o frodi, diverse da quelli presidiati dalle attività di controllo. La valutazione di tali controlli si basa sull'analisi di fattori tangibili (quali, policy e procedure) e fattori intangibili (come la filosofia aziendale e il *modus operandi* del management).
La valutazione degli Entity Level Control risulta quindi essere uno step strategico per la comprensione e la valutazione del sistema di controllo interno di un'azienda, rispecchiando direttamente l'atteggiamento, la consapevolezza e le azioni del management relativamente alla creazione ed all'esecuzione dei controlli applicati sui processi aziendali.
Oltre ad essere applicabili quindi alle differenti attività di business di un'azienda, questi controlli, agiscono anche sui processi in ambito IT, andando a creare i presupposti dell'operatività di quei controlli più "atomici" quali:

- gli IT General Controls, che agiscono al livello di "attività",
- gli Application Controls, specifici degli applicativi di business.

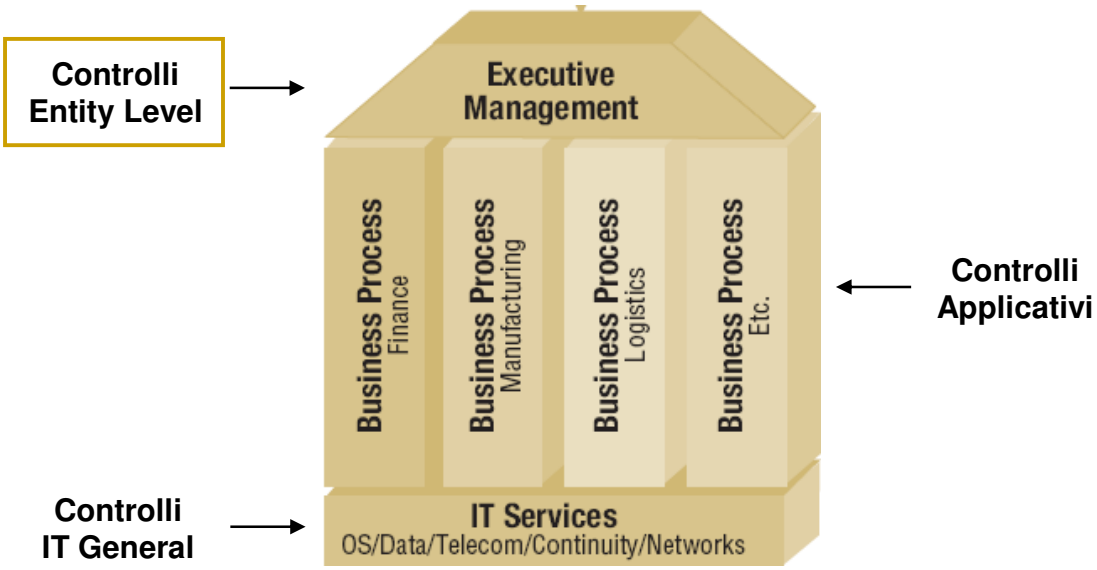


Fig. 1

I controlli entity-level, dunque, si riflettono nello stile operativo dell'organizzazione e comprendono politiche, procedure e altre prassi di alto livello che definiscono l'ambiente operativo generale in azienda. La presenza di forti controlli IT entity-level, quali politiche ben definite e comunicate, può indicare che ci si trova di fronte ad un ambiente operativo IT affidabile. Analogamente, aziende con controlli IT entity-level deboli sono spesso in difficoltà nello sviluppare un programma di controlli coerente. In sintesi la debolezza o robustezza dei controlli entity-level gioca un ruolo rilevante sulla natura, l'estensione e il timing delle attività di test.

Sulla rilevanza di questi controlli, si esprime il PCAOB con l'Auditing Standard N°5:

> *[…] Entity-level controls vary in nature and precision. Some entity-level controls, such as certain control environment controls, have an important, but indirect, effect on the likelihood that a misstatement will be detected or prevented on a timely basis. These controls might affect the other controls the auditor selects for testing and the nature, timing, and extent of procedures the auditor performs on other controls.*

Il PCAOB afferma, inoltre, che un ambiente di controllo inefficace deve essere interpretato come una mancanza grave e come sintomo che esiste una concreta debolezza nel sistema di controllo interno sul financial reporting. Queste osservazioni sono applicabili a qualunque ambito di controllo, incluso quello IT.

I modelli di controllo interno di riferimento raccomandati [5] dalla presente guida sono:

- Internal Control — Integrated Framework: è lo standard internazionale più noto e diffuso per il sistema di controlli interni, pubblicato nel 1992 dal Committee of Sponsoring Organizations of the Treadway Commission (COSO); tale standard, negli USA, è stato indicato come guideline per la conformità al Sarbanes-Oxley Act dal SEC, l'organo di controllo della borsa;

- IT Control Objectives for Sarbanes-Oxley: pubblicato nel 2004 dall'ISACA ed aggiornato nel settembre 2006 (sulla base delle nuove guidelines SEC e PCAOB relative agli entity level control, all'approccio risk based/top down, agli application control ed alla valutazione delle debolezze), fornisce un approccio coerente per gli aspetti relativi agli obiettivi di controllo IT, sulla base del framework COSO.

[5] La guida riconosce che altri modelli di controllo sono ammissibili, purchè presentino caratteristiche comparabili nella sostanza alle 5 componenti del COSO (par. 1.1).

3.1.1 COSO

Al fine di ottenere un controllo interno efficace, COSO ritiene necessaria la presenza di controlli IT affidabili per le sue cinque componenti:

- Ambiente di controllo;
- Risk Assessment;
- Attività di controllo;
- Informazione e Comunicazione;
- Monitoraggio.

Queste componenti, ad eccezione della componente “Attività di controllo”, che risulta specificamente orientata ai Controlli Generali e ai Controlli Applicativi, risultano rilevanti a livello di entità.

3.1.1.1 Ambiente di controllo

L’ambiente di controllo è il punto di partenza e la base per stabilire un controllo interno efficace in quanto definisce il "tone-at-the-top"[6]. Le tematiche affrontate in questa componente si applicano trasversalmente a tutta l’azienda. L’ambiente di controllo è una problematica di tipo aziendale, cioè di tipo entity-level, in quanto ormai l’IT ha assunto caratteristiche che richiedono l’attenzione del management sull’allineamento dei sistemi agli obiettivi di business, sui ruoli e sulle responsabilità, sulle politiche, sulle procedure e sulle competenze tecniche.

3.1.1.2 Risk Assessment

Il Risk Assessment consiste nell’identificazione da parte del management dei rischi che possono compromettere il raggiungimento degli obiettivi aziendali; insieme ai rischi il management deve identificare anche le relative attività di controllo. È probabile che i rischi in ambito di controllo interno siano diffusi nelle funzioni IT più che nelle altre aree. Il risk assessment può essere effettuato, oltre che a livello di attività (*activity-level*, per uno specifico processo o business unit), a livello di entità (*entity-level*, per tutta l’organizzazione nel suo complesso), in modo da cogliere gli aspetti di trasversalità dei rischi rispetto a funzioni e processi (ad es. IT management, Information Security).

[6] Espressione con cui il COSO riassume il massimo livello qualitativo atteso nel sistema di controllo

3.1.1.3Informazione e comunicazione

COSO recita che le informazioni sono necessarie a tutti i livelli dell'organizzazione per permettere il raggiungimento degli obiettivi di business e garantire il perseguimento degli obiettivi di controllo generali a livello di entità. Lo sviluppo di Corporate Policy, nonché l'identificazione, gestione e comunicazione delle informazioni più rilevanti sono le caratteristiche distintive di questa componente che assume particolare rilievo in relazione al processo di financial reporting.

3.1.1.4Monitoraggio

Il monitoraggio, che comprende:

a) la supervisione dei controlli interni da parte del management attraverso un processo di assessment periodico;
b) L'audit interno;

è sempre più importante per l'IT management. In maniera sempre maggiore, la performance e l'efficacia dell'IT sono monitorate e misurate.

3.1.2 IT Control Objectives for SOX (COBIT® FOR SOX)

L'IT Control Objectives for SOX presenta un approccio agli Entity Level Controls che integra COBIT® e COSO, incrociati lungo le loro dimensioni fondamentali. A riguardo, risulta particolarmente interessante la mappatura dei due framework, rappresentata nella tabella seguente:

			Componenti COSO				
Entity level	Activity Level	**Processi IT COBIT®**	Ambiente di controllo	Risk Assessment	Attività di controllo	Informazione e comunicazione	Monitoraggio
Pianificazione e (ambiente IT)							
•		Definizione della pianificazione strategica IT		•		•	•
		Definizione della architettura informativa					
		Determinazione della direzione tecnologica					
•		Definizione dei process IT, dell'organizzazione e delle relazioni	•			•	•
		Gestione degli investimenti IT					
•		Comunicazione degli obiettivi e della direzione	•			•	
•		Gestione delle risorse umane IT	•			•	
•		Gestione della qualità	•		•	•	•
•		Valutazione e gestione dei rischi IT		•			
		Gestione dei progetti					
Acquisizione ed Implementazione (sviluppo dei programmi e Change Program)							
		Identificazione delle soluzioni automatizzate					

	•	Acquisizione e manutenzione del software applicativo			•		
	•	Acquisizione e manutenzione della infrastruttura tecnologica			•		
	•	Abilitazione delle operazioni e uso			•	•	
		Procure IT resource					
	•	Gestione del cambiamento		•	•		•
	•	Installazione e validazione di soluzioni e cambiamenti			•		
Delivery e supporto (procedure informatiche ed accesso a programmi e dati)							
	•	Definizione e gestione dei livelli di servizio	•		•	•	•
	•	Gestione dei servizi delle terze parti	•	•	•		•
		Gestione delle performance e della capacità					
		Assicurare servizi continui					
	•	Assicurare la sicurezza dei sistemi			•	•	•
		Identificare ed allocare i costi					
•		Formare e informare gli utilizzatori	•			•	
	•	Gestire l'help desk e gli incidenti			•	•	•
	•	Gestire la configurazione			•	•	
	•	Gestire i problemi			•	•	•
	•	Gestire i dati			•	•	
	•	Gestire l'ambiente fisico			•	•	
	•	Gestire le procedure			•	•	
Monitoraggio e valutazione (ambiente IT)							
•		Monitoraggio e valutazione delle performace IT			•	•	•
•		Monitoraggio e valutazione del controllo interno	•				•
•		Assicurare la compliance alle norme			•	•	•
•		Assicurare l'it Governance	•				•

Fonte: ITGI - COBIT® for Sarbanes

Tab. 1

Raccordo COSO, COBIT® FOR SOX, VIGILANZA BANKIT

COBIT® FOR SOX	**COSO**	**BANKIT**
	MONITORING	**AUDIT & CORPORATE AUDIT = CONTROLLI DI 3° E 4° LIVELLO**
ELC	CONTROL ENVIRONMENT	CONTROLLI DI SUPERVISIONE E RISK ASSESSMENT = CONTROLLI DI 2° LIVELLO
	RISK ASSESSMENT	
	INFORMATION & COMMUNICATION	
ALC	ATTIVITA' DI CONTROLLO	CONTROLLI DI LINEA = CONTROLLI DI 1° LIVELLO

Sintetizzando, con le parole dell' IT Control Objectives for Sarbanes-Oxley, possiamo dire che gli Entity Level Controls riguardano:

- Strategie e Piani;
- Politiche e Procedure;
- Attività di valutazione del Rischio;
- Addestramento e Formazione;
- Assicurazione della Qualità;
- Audit Interni.

Fermo restando il principio che non è possibile identificare un approccio "valido" in ogni circostanza e per ogni azienda, ed essendo necessario che ognuno realizzi un proprio modello di obiettivi di controllo che tenga conto delle proprie specifiche caratteristiche, l'IT Control Objectives for SOX suggerisce dei punti di analisi adottabili al livello di entità (Entity Level Controls) che si focalizzano sui seguenti ambiti:

- Piani strategici IT: relativamente ai meccanismi di predisposizione, comunicazione e monitoraggio;
- Processi IT, Organizzazioni e relazioni: a livello di corretta assegnazione e segregazione di ruoli e responsabilità;
- Gestione delle risorse umane IT, con riferimento alla cultura aziendale e al codice etico;
- Formazione e training degli utenti;
- Comunicazione chiara e tempestiva delle direttive dell'Alta Direzione da impartire al management, in modo da assicurare il perseguimento degli obiettivi aziendali;
- Valutazione attraverso un adeguato risk assessment e gestione dei rischi IT;
- Gestione della qualità;
- Monitoraggio e valutazione delle performance;
- Monitoraggio e valutazione del controllo interno.

3.2 IT General Control

3.2.1 Definizione e caratteristiche

Gli IT General Control (*ITGC*) costituiscono le fondamenta di un modello di controllo dei sistemi informativi. L'obiettivo degli ITGC è di fornire una valutazione della struttura organizzativa, operativa e gestionale dei sistemi informativi, al fine ultimo di assicurare l'affidabilità delle informazioni gestite.

I controlli generali servono quindi per capire come i sistemi informativi operano, come sono organizzati, quali sono le politiche e le procedure adottate per lo sviluppo del software, per la gestione della sicurezza, dei cambiamenti all'organizzazione, al software, alla sicurezza e per garantire la continuità dei servizi IT.

Questi controlli sono definiti di carattere “generale” per distinguerli da quelli “applicativi” (*IT Application Controls*) che sono completamente automatizzati e le cui logiche sono “cablate” nei programmi.

La validità dei controlli generali è condizione necessaria ancorchè non sufficiente per una corretta operatività dei controlli applicativi, così come la validità dei controlli Entity Level (*ELC*), definendo i principi e le linee guida IT in sinergia con le strategie di business, è necessaria per una corretta definizione dei controlli generali.

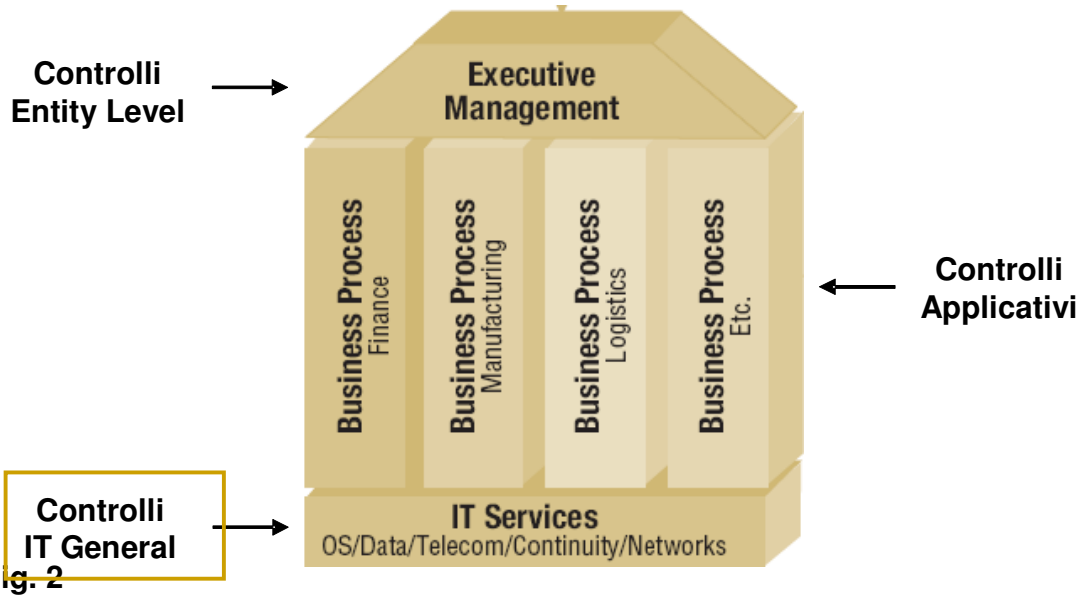


Fig. 2

I controlli generali solitamente coprono aree come:

- Gestione della sicurezza: politiche, procedure, organizzazione, misure preventive, monitoraggio;
- Gestione dei cambiamenti (Change management): sia applicativo che dei sistemi;
- Ciclo di vita del software (Software Development Life Cycle);
- Gestione dei dati: interfacce, amministrazione, qualità;
- Gestione degli incidenti: operativi e di sicurezza;
- Gestione operativa e dei problemi (Technical Support);
- Gestione della continuità dei servizi e dei backup;
- Analisi dei rischi e controlli interni (se non trattati nei controlli Entity Level).

La selezione dei processi IT da verificare e la conseguente definizione degli obiettivi di controllo[7], dipendono dalla:

- L'analisi dei rischi dei sistemi informativi che dovrà essere aggiornata e dettagliata;
- La disponibilità di una corretta mappatura tra processi di business e le applicazioni utilizzate;

[7] Si definisce obiettivo di controllo la finalità che deve essere perseguita e soddisfatta nel disegno e nell’esecuzione di attività di controllo.

- La Metodologia adottata;
- La conoscenza di standard, framework internazionali o best practice di riferimento.

Nei paragrafi seguenti da 2.1.1. a 2.1.5. sono fornite le linee guida utili per un primo impianto di un sistema di controlli conformi alla Legge 262/2005 o per la valutazione dell'estensione delle attività di testing che devono essere effettuate in applicazione della Legge.

Di seguito sono in premessa illustrati i ruoli e le responsabilità per una corretta implementazione del modello.

3.2.1.1 Attribuzione di ruoli e responsabilità di controllo

All'inizio della definizione del modello di controllo è necessario formalizzare i ruoli coinvolti e le relative responsabilità in accordo con l'organizzazione delle business unit.
In particolare è consigliabile definire i seguenti ruoli:

- il process owner: responsabile del processo IT sotto il profilo degli obiettivi aziendali perseguiti, efficacia ed efficienza delle relative procedure e risorse assegnate. Il process owner identifica i control owner (responsabili di controllo) delegati allo svolgimento dei singoli controlli, prende visione dei risultati e conferma la sistemazione o correzione (remediation) del proprio processo;
- il control owner: responsabile di uno o più controlli specifici (di I° livello), supporta i verificatori (tester) durante le attività di audit, convalida i risultati del test, può partecipare alla stesura delle remediation;
- il soggetto responsabile delle attività di remediation;
- il rappresentante della direzione IT che riceverà e prenderà visione sia del risultato finale degli audit, sia del piano d'azione conclusivo.

3.2.1.2 Linee guida per lo studio e la definizione degli obbiettivi di controllo

Nella selezione degli obiettivi di controllo occorre ricordare che l'oggetto della normativa è il financial reporting, pertanto i controlli devono coprire l'intero ciclo di vita delle informazioni e dei dati che lo compongono.
I controlli devono inoltre fornire la garanzia che, se correttamente effettuati, le informazioni necessarie per il financial reporting siano affidabili nei confronti degli investitori, degli stakeholder, del management e delle autorità di controllo.
Come premessa necessaria a questa sezione è importante ricordare che non può esistere alcuna garanzia che un insieme predefinito di controlli sia sufficiente per assicurare l'affidabilità dei dati finanziari e che quindi è necessaria una valutazione attenta delle aziende per identificare le aree con il rischio maggiore.
Pertanto le linee guida successive sono da ritenersi delle indicazioni di massima per le valutazioni che rimangono in carico alle singole società.

I passi principali per la definizione degli obbiettivi di controllo:

- Identificazione dei processi COBIT®;

- Identificazione degli obiettivi di controllo all'interno dei processi selezionati;
- Valutazione delle priorità degli obiettivi di controllo selezionati.

Per identificare i processi COBIT® è possibile:

- utilizzare come supporto il documento IT Control Objectives for SOX;
- utilizzare gli Information Requirements del COBIT®;
- integrare i due riferimenti di cui sopra con le attività di analisi dei rischi effettuate dalle singole società.

Nella tab. 1, tratta da l'IT Control Objectives for SOX, si possono osservare i 14 processi COBIT® associati a "Activity Level Controls", raccordati con le componenti COSO.

I processi marcati come Activity Level sono da considerarsi una base di partenza per la definizione dei processi dai quali selezionare i control objectives che andranno a costituire il set ITGC.

Per utilizzare il supporto degli Information Requirements occorre considerare i seguenti requisiti per i dati:

- Riservatezza;
- Integrità;
- Disponibilità;
- Conformità;
- Affidabilità.

Tali requisiti interessano 25 dei 34 processi del COBIT® e possono essere valutati considerando il relativo obiettivo primario "P" o secondario "S" nei rispetti di ciascun criterio informativo.

	BUSINESS PROCESS								
	IT PROCESS			**OPERATIONS PROCESS**					
	EFFICIENCY CONTROLS	**EFFECTIVENESS CONTROLS**		**PAY**	**PRODUCTION**	**LOGISTICS**	**SALES**	**PURCHASING**	**OTHER**
		ENTITY LEVEL CONTROL	ACTIVITY LEVEL CONTROL	AC	AC	AC	AC	AC	AC
IT CONTROLS	9 PROCESS	11 PROCESS	14 PROCESS						
OPERATIONS CONTROL	X			X	X	X	X	X	X
REPORTING CONTROL	X	X	X	X	X	X	X	X	X

La tabella sottostante riporta l'elenco dei processi COBIT® in relazione ai criteri informativi.

		Criteri Informativi						
DOMINIO	**PROCESSO IT**	Efficacia	Efficienza	Riservatezza	Integrità	Disponibilità	Conformità	Affidabilità
PO	PO1 Definizione di un piano strategico IT	P	S					
	PO2 Definizione di un'architettura informatica	S	P	S	P			
	PO3 Determinazione dell'orientamento tecnologico	P	P					
	PO4 Definizione di processi, organizzazione e relazioni IT	P	P					
	PO5 Gestione degli investimenti IT	P	P					S
	PO6 Comunicazione degli obiettivi e dell'orientamento della direzione	P					S	
	P07 Gestione delle risorse umane IT	P	P					
	PO8 Gestione della qualità	P	P		S			S
	PO9 Valutazione e gestione dei rischi IT	S	S	P	P	P	S	S
	PO10 Gestione dei progetti	P	P					
DS	DS1 Definizione e gestione dei livelli di servizio	P	P	S	S	S	S	S
	DS2 Gestione dei servizi delle Terze parti	P	P	S	S	S	S	S
	DS3 Gestione delle prestazioni e dei volumi	P	P			S		
	DS4 Garanzia della continuità del servizio	P	S			P		
	DS5 Garanzia della sicurezza dei sistemi			P	P	S	S	S
	DS6 Identificazione ed allocazione dei costi		P					P
	DS7 Istruzione e formazione degli utenti	P	S					
	DS8 Gestione di un ufficio per la gestione del servizio e degli incidenti	P	P					
	DS9 Gestione della configurazione	P	S			S		S
	DS10Gestione dei problemi	P	P			S		
	DS11 Gestione dei dati				P			P
	DS12 Gestione del ambiente fisico				P	P		
	DS13 Gestione dell'operatività	P	P		S	S		
AI	AI1 Identificazione di soluzioni automatizzate	P	S					
	AI2 Acquisizione e manutenzione di software applicativo	P	P		S			S
	AI3 Acquisizione e manutenzione di infrastruttura tecnologica	S	P		S	S		
	AI4 Abilitazione all'operatività ed all'utilizzo	P	P		S	S	S	S
	AI5 Approvvigionamento delle risorse IT	S	P				S	
	AI6Gestione dei cambiamenti	P	P		P	P		S
	AI7 Installazione ed autorizzazione di soluzioni e variazioni	P	S		S	S		
ME	ME1 Verifica e valutazione delle prestazioni IT	P	P	S	S	S	S	S
	ME2 Verifica e valutazione del controllo interno	P	P	S	S	S	S	S
	ME3Garanzia di conformità alle normative						P	S
	ME4 Garantire il governo dell'IT	P	P	S	S	S	S	S

Tab. 2

Questi criteri informativi esprimono il concetto che il dato effettivo (gestito dai sistemi applicativi in ambiente di produzione) sia garantito a partire dal suo punto di ingresso nei sistemi, fino alla sua partecipazione ad un'informazione finanziaria, che sia essa un report, un grafico o qualsiasi altra forma di utilizzo. Inoltre, il dato non deve essere alterato o in genere utilizzato né direttamente né tramite transazioni applicative, se non da persone autorizzate a farlo. In pratica è necessario tracciare "chi-fa-cosa" e perché.[8]

[8] Tale esigenza deve essere bilanciata con la prescrizione dell'art. 4 della Legge 300/71 (Statuto dei lavoratori) che vieta il controllo a distanza dei lavoratori. Il bilanciamento è ottenuto applicando regole esplicite di controllo, connesse e proporzionate a finalità aziendali legittime e condivise con le rappresentanze dei lavoratori o in caso di disaccordo approvate dalla Direzione Provinciale del Lavoro o Ente equivalente.

Nonostante i criteri informativi si applichino ai dati trattati dai sistemi applicativi, essi per taluni aspetti (integrità nello sviluppo e manutenzione del software, integrità dei dati trattati e della produzione, sicurezza degli accessi) si applicano anche ai Processi IT sottostanti i sistemi applicativi.

Per questo motivo è importante coprire l'intero ciclo dei sistemi informativi, in quanto ogni processo ha le sue particolarità ed i suoi rischi inerenti.

Ad esempio, nello sviluppo applicativo è necessario verificare la corrispondenza tra le funzionalità richieste dagli utenti e quelle realizzate, per evitare operazioni sui dati fraudolente o a rischio per l'integrità delle informazioni.

Sempre come esempio, nella gestione dei cambiamenti è importante verificare che i controlli di 1° livello garantiscano che ogni cambiamento applicativo, di configurazione o di sistema, sia giustificato, richiesto, autorizzato e documentato.

Particolare rilevanza assumono i cambiamenti o gli interventi in emergenza, perché solitamente vengono eseguiti con procedure che "vanno in deroga" ai normali controlli ed ai flussi autorizzativi e sono operati spesso con dei profili di sistema che dispongono di alti privilegi, pertanto sono difficilmente tracciabili.

Come citato, è anche possibile effettuare una valutazione comparata utilizzando sia le indicazioni relative alla selezione dei processi Sarbanes-Oxley, sia le indicazioni relative ai criteri informativi dei singoli processi.

Nell'Appendice II del COBIT® 4.1, si possono osservare i processi IT e le relative caratteristiche in relazione alle componenti COSO ed agli *Information Requirements*.

Le attività di analisi del rischio, effettuate dalle singole società, possono integrare lo studio dei processi da sottoporre a verifica aggiungendo o eliminando processi sulla base delle risultanze.

L'identificazione dei singoli obiettivi di controllo costituisce un procedimento che può essere molto complesso. Gli elementi per la valutazione dei singoli obiettivi sono molteplici e sfruttano la conoscenza dell'azienda dei propri sistemi informativi, delle relative criticità, dell'organizzazione IT, dello stato di completezza ed applicazione delle politiche e delle procedure IT, della professionalità e della formazione delle risorse, dell'analisi dei rischi ed altro ancora.

Una lista dei possibili obiettivi di controllo si può trovare nelle figure dalla 15 alla 27 del documento l'IT Control Objectives for SOX.

Per facilitare la comprensione degli obbiettivi di controllo da parte sia dei control owner che dei verificatori (per le attività di audit), è consigliabile valutare la possibilità di separare un singolo obiettivo di controllo in obiettivi più atomici.

Ad esempio, al posto di: "*La politica di sicurezza dei sistemi informativi deve essere formalizzata e coerente con le best practice, approvata dal management, conosciuta e diffusa da tutto il personale IT*", potrebbero essere ricavati tre obiettivi più semplici:

- *"La politica di sicurezza dei sistemi informativi deve essere formalizzata e coerente con le best practice"*: dove può essere verificata la coerenza dei contenuti con lo standard ISO/IEC 27001;
- *"La politica di sicurezza dei sistemi informativi deve essere approvata dal management"*: dove può essere verificata l'evidenza scritta che attesta la data di approvazione del documento (ad esempio un verbale);
- *"La politica di sicurezza dei sistemi informativi deve essere conosciuta e diffusa a tutto il personale IT"*: dove può essere verificata la modalità di presa visione da parte del personale e le evidenze del training sostenuto dal personale.

Nel caso in cui il framework degli obiettivi di controllo venga valutato da gruppi di IT auditor (tester) diversi è consigliabile affiancare a ciascun obiettivo di controllo delle "audit guidelines" ricavate da quelle del COBIT® o da altre best practice e standard di riferimento.

3.2.1.3Criteri per l'identificazione delle "aggregazioni" e/o layer IT di osservazione degli obiettivi di controllo

Durante la definizione del framework degli obiettivi di controllo è opportuno considerare a quali applicazioni sarà applicato. Nella definizione dell'ambito viene solitamente considerato come un unico livello, a cui applicare gli obiettivi di controllo, l'insieme di applicazioni che risponde a criteri di gestione omogenei o caratteristiche tecnologiche comuni.

Ad esempio, se i file server Windows sono relativi a sistemi applicativi inclusi nell'ambito del progetto (vedasi cap. 2) e se la loro gestione è governata dagli stessi processi IT e operata dalla stessa business unit, allora il set dei controlli potrà essere svolto una volta sola dallo stesso gruppo di persone.

Un altro esempio consiste nel verificare se le procedure del ciclo di vita del software sono comuni a tutti i gruppi di sviluppo applicativo oppure se ciascun gruppo può definire o personalizzare le proprie procedure operative. Nel primo caso è possibile effettuare un test del disegno delle procedure comuni e svolgere un test di efficacia campionando i progetti dei diversi gruppi di lavoro; nel secondo caso occorrerà invece ripetere sia il test del disegno che quello di efficacia per ciascun gruppo di sviluppo che si occupi delle applicazioni incluso nell'ambito del progetto.

Come ulteriore esempio si può considerare che spesso l'analisi delle politiche di sicurezza e le tematiche di business continuity possono essere gestite in modo trasversale rispetto alle business unit dallo stesso gruppo di lavoro. In questo caso alcuni dei controlli relativi al processo di gestione della sicurezza potranno essere svolti centralmente con valenza generale.

Pertanto, dopo la definizione del framework, si prevede un'attività di analisi dei gruppi che gestiscono le applicazioni incluso nell'ambito del progetto, per capirne l'effettiva organizzazione e la relativa area di competenza rispetto ai processi IT identificati.

A fronte di questa analisi è possibile stimare con maggior precisione la quantità di risorse necessaria per lo svolgimento dei test.

3.2.1.4Requisiti normativi critici

Qualora la società operi un business soggetto a particolari normative di settore (ad es. le società di Public Utilities (ex Municipalizzate, società di servizi, società per la riscossione dei tributi, ecc.), gli operatori di servizi telefonici, di servizi di hosting & housing di sistemi, etc), è importante:

- verificare se tali normative offrono una sinergia (efficienza) con il modello dei controlli definito;
- verificare l'impatto della violazione di tali normative in termini di sanzioni amministrative o altri impatti sui controlli definiti.

Pertanto è possibile considerare le normative tipiche dello specifico business aziendale, sia come possibile sinergia di analisi, sia come elemento critico per valutare la compliance normativa ed i rischi.

3.2.1.5Integrazione con framework, standard e best practice di riferimento

Nella definizione degli obiettivi di controllo è importante considerare il coordinamento con altri standard e/o best practice internazionali quali ISO27001 e ITIL v3, che rappresentano i framework più diffusi. Da tale coordinamento possono scaturire opportunità di estensione e integrazione delle modalità di controllo.

Lo standard ISO 27001 può essere utilizzato principalmente per integrare i processi relativi a:
- definizione delle politiche di sicurezza;
- sicurezza logica e fisica;
- continuità ed al backup dei sistemi.

La best practice ITIL v3 può essere utilizzata principalmente per integrare i processi relativi a:
- gestione dei cambiamenti (change management);
- test ed al rilascio degli aggiornamenti;
- supporto agli utenti;
- esercizio dei sistemi;
- gestione dei problemi e degli incidenti.

L'integrazione tra COBIT® 4.1, ITIL v3 e ISO27001, pur richiedendo un'attenta analisi degli obiettivi e una conoscenza della struttura dei sistemi informativi da analizzare, può consentire di ottenere risultati migliori in termini di copertura del rischio e del dettaglio del controllo.

Nella tabella sottostante si illustra un esempio di come gli obiettivi di controllo identificati possono essere rappresentati assieme ai riferimenti esterni che li collegano ai rispettivi framework, standard o best practice di origine.

MACRO PROCESS	PROCESS	CONTROL OBJECTIVE	EXTERNAL REFERENCE
Change Management	Pianificazione dei cambiamenti	La pianificazione dei cambiamenti è documentata e tutti i cambiamenti sono soggetti a formale procedura di approvazione da parte del committente e da parte del Change Manager.	COBIT® AI6.2, AI7.3, ITIL Service Transition 6.2 (Change Management), ISO27001 10.1.2, 12.5.1
Change Management	Test delle modifiche	La verifica delle modifiche avviene tramite test di collaudo in ambiente/i separati da quello di produzione da parte del personale IT preposto e dal committente (se ci sono impatti funzionali). I risultati dei test effettuati sono documentati.	COBIT® AI7.4, ISO27001 A.12.5.1, A.10.1.4; ITIL Service Transition 6.5 (Service validation and Testing releases)

Tab. 3

Nel caso di realtà aziendali strutturate, con una capogruppo e delle società controllate, è necessario verificare l'omogeneità degli standard e/o le best practice adottati dai diversi gruppi di lavoro.

3.2.1.6 Assegnazione per finalità di "testing" delle priorità e delle caratteristiche dei controlli

Richiamando l'esperienza relativa alla normativa Sarbanes-Oxley nella quale si definiscono dei controlli chiave, similmente è possibile definire priorità e caratteristiche dei controlli.

Come già detto, la valutazione delle singole società è un elemento importante nella definizione delle priorità dei controlli pur se supportata da indicazioni derivate da best practice internazionali.

Si possono osservare alcuni modelli comunemente usati per l'assegnazione delle priorità dei controlli:

- priorità basata su una scala qualitativa (ad es. alto-medio-basso);
- priorità basata su una scala o un elemento quantitativo (ad es. una percentuale di probabilità, una valorizzazione dell'impatto, etc.);
- priorità basata su un'analisi del rischio residuo;
- priorità basata sul concetto di controllo chiave o non chiave.

Tutti questi metodi di classificazione offrono la possibilità sia di comporre una valutazione finale del rischio residuo strutturata con un calcolo specifico, sia di poter definire un metodo di analisi che porti a delle efficienze a fronte di un possibile approccio graduale o per fasi successive.

3.2.1.7Formalizzazione (documentazione) del "testing" dei controlli

Un progetto ITGC 262 può raccogliere le evidenze di decine o centinaia di test. La documentazione necessaria è generalmente è composta da:

- Executive Summary con la metodologia di testing utilizzata, l'ambito del progetto, il modello di controllo ed i risultati;
- Dettaglio dei test: schede di test con dettaglio delle evidenze;
- Allegati: repository delle evidenze catalogate.

Nell'organizzazione del repository per le evidenze è importante ricordare che il volume dei documenti raccolti potrebbe essere considerevole, in quanto per ogni test che preveda una campionatura si dovrà archiviare il campione di item selezionato, purchè sia sempre ricostruibile l'intera popolazione da cui il campione è stato estratto.

3.3 L'outsourcing dei servizi IT e il sistema dei controlli interni

Molte aziende trasferiscono presso un fornitore di servizi una porzione delle loro attività operative, incluso i servizi del proprio sistema informativo (servizi IT)[9].

Ai fini della conformità con la Legge 262/2005 un servizio IT risulta rilevante quando impatta in uno dei seguenti ambiti:

- sull'insieme delle transazioni/movimenti del cliente che sono significative per la predisposizione del bilancio;
- sulle procedure, sia automatiche che manuali, per mezzo delle quali le transazioni/movimenti del cliente sono iniziate, registrate, processate e rappresentate, dal loro verificarsi alla loro inclusione nel bilancio;

[9] Dove con "Servizio IT" si intende il risultato dell'insieme di processi informatici svolti da una organizzazione (in questo caso un "Outsourcer"), per un dato periodo, al fine di soddisfare le esigenze di un committente.

- sulle modalità con cui vengono catturati ulteriori eventi e condizioni che sono significativi per la relazione di bilancio;
- sulle modalità di gestione delle scritture contabili e sul processo di generazione del bilancio.

Quando un servizio erogato da un outsourcer è ritenuto rilevante ai fini della conformità con la Legge 262/2005 esso deve essere considerato nell'ambito del sistema di controllo interno disegnato ai fini della predisposizione del bilancio di esercizio e il management dell'organizzazione ha la responsabilità di valutare il disegno e l'efficacia operativa del sistema di controllo interno adottato dall'outsourcer secondo modalità equivalenti a quelle seguite per i processi IT svolti internamente all'azienda.

Nella determinazione dell'efficacia del sistema di controllo interno dell'outsourcer, ciò nondimeno, si deve tener conto di diversi fattori fra cui:

- informazioni disponibili sull'outsourcer e sul suo sistema di controllo interno;
- l'impatto che i rischi associati al sistema di controllo interno dell'outsourcer hanno sul bilancio dell'azienda cliente;
- la natura e la complessità del servizio erogato (standardizzazione, dimensione degli utenti, etc.) dall'outsourcer;
- l'estensione dell'interazione fra i due sistemi di controllo;
- l'applicazione di controlli lato utente relativamente ad attività effettuate dalla società o centro di servizi (Service Organization);
- i termini contrattuali che regolano gli accordi fra utente ed erogatore del servizio a livello di individuazione di responsabilità, libertà decisionale concessa, individuazione di KPI (Key Performance Indicator) e misurazione, penalità previste, clausola di auditabilità, etc.

3.3.1 La modalità di controllo dell'Outsourcer

Per i servizi IT esternalizzati per i quali deve essere previsto un sistema di controllo interno, l'organizzazione soggetto alla Legge 262/2005 deve prevedere procedure che consentano di:

- ottenere un'adeguata descrizione dei controlli implementati dall'outsourcer ai fini della comprensione del livello di mitigazione del rischio;
- ottenere evidenza che i controlli predisposti dall'outsourcer siano operanti.

L'evidenza che i controlli siano operanti può essere ottenuta:

- richiedendo un "Service Auditor's report" (si veda di seguito) sui controlli implementati presso l'outsourcer;
- effettuando un "Test of Controls" direttamente presso l'outsourcer.

In tale ambito si pone il problema del rapporto tra quanto riportato come risultato di audit interni o esterni precedentemente effettuati da altri "Service Auditor" presso l'Outsourcer e l'ambito richiesto dall'azienda cliente in qualità di "User Organization" (e cioè responsabile della verifica dell'adozione dei controlli da parte dell'outsourcer).

Mentre in linea generale l'outsourcer può produrre qualsivoglia evidenza delle risultanze degli audit passati o dei processi atti a garantire l'allineamento alle politiche di gestione del rischio (adottate nell'erogazione dei servizi, allo scopo di dimostrare l'esistenza e l'efficace applicazione dei controlli interni), lo "User Auditor" (in questo caso l'organizzazione soggetta alla Legge 262/2005) può evidentemente chiedere a sua volta di poter eseguire nuovi test sul campo allo scopo di verificarne l'esistenza e l'efficacia nel periodo temporale che corrisponde al periodo coperto dal bilancio a cui si devono riferire i controlli.

Il ruolo del Service Auditor e l'attestazione SAS 70

Con "Service Auditor" si intende generalmente l'organizzazione indipendente di revisione a cui un'azienda di Servizi IT conferisce l'incarico di sottoporre ad Audit una componente della propria organizzazione.

La scelta di un Outsourcer di conferire un tale incarico di revisione risponde normalmente ad una logica di attestazione del positivo superamento di una revisione basata su criteri standard, effettuata da una terza parte indipendente e codificata secondo formalismi accettati dalla comunità delle società di auditing.

Il punto di vista di un Auditor Esterno:

L'attestazione SAS 70[10] è perseguita dal Service in funzione della necessità di rappresentare in modo oggettivo ai propri clienti il livello di controllo interno che il Service esercita nell'erogare il servizio al cliente. La standardizzazione sia delle modalità dell'esame che della relazione finale dell'esito sono di norma accettate dall'Auditor del cliente, sia interno che esterno ("User Auditor"), permettendo a questo di acquisire tale attestazione in modo formale nell'ambito della valutazione del sistema di controllo interno (SCI) del Service.

Esistono due tipologie di report SAS 70:

A) "Report type I" che include una descrizione del sistema dei controlli dell'azienda e l'opinione dell'auditor indipendente riguardo:

- la copertura degli obiettivi di controllo dichiarati da parte del modello dei controlli aziendali.

B) "Report type II" che include il Report type I e il test dell'efficacia dei controlli in un arco temporale (da un minimo di 6 mesi all'intero periodo di bilancio) per fornire una ragionevole, ma non assoluta assicurazione, che gli obiettivi di controllo siano stati raggiunti.

[10] Il SAS 70 è il principio di revisione americano a cui corrisponde, nell'ambito dei principi di revisione internazionali, l'ISA 402

La disponibilità per l'outsourcer di un "Report type II" del SAS 70, che comporta successive osservazioni e regolari scadenze temporali, mette a disposizione dell'azienda cliente (organizzazione soggetta alla Legge 262/2005) la possibilità di utilizzare le attestazioni relative al livello dei controlli interni dell'outsourcer a complemento di quelle relative ai propri.

Tale report, redatto e rilasciato da un "Service Auditor" indipendente, fornirebbe al proprio auditor la documentazione di una revisione condotta secondo uno standard effettivamente orientato alla comunicazione tra diversi Auditor e specializzato alle aziende di erogazione dei Servizi IT.[11]

In particolare, l'ottenimento di un SAS 70 Report type II da un Service Auditor, permette di determinare il grado di affidamento ottenuto sul sistema di controllo dell'outsourcer. Tale valutazione può determinare una riduzione dell'estensione delle attività di test sia di conformità che di sostanza effettuate dallo User Auditor, relativamente alle aree coperte dal report stesso. Tale valutazione va svolta avendo cura di confrontare gli obiettivi di controllo indirizzati dal SAS 70 con quelli per cui si ritiene necessario ottenere affidamento. Eventuali obiettivi di controllo non coperti andranno indirizzati con –alternativamente- l'estensione del SAS 70 o con altre procedure.

3.3.2 Il ruolo del contratto di outsourcing

Il contratto di servizio e i relativi accordi annessi costituiscono la base normativa sulla quale costruire le modalità di svolgimento dell'audit.

Il massimo beneficio ottenibile mediante un audit del SCI dell'outsourcer potrà essere conseguito mantenendone tutto lo svolgimento nell'ambito di ben determinate procedure preliminarmente condivise tra l'outsourcer e l'organizzazione cliente soggetta alla Legge 262/2005 e regolando in modo formale qualsiasi eventuale attività aggiuntiva che fosse richiesta da auditor di terze parti.

La protezione delle informazioni proprie e dei clienti (incluso il committente dell'Audit) sarà conseguita permettendo l'accesso dello "User Organization" alle informazioni attinenti il perimetro dell'Audit stesso, nel rispetto del divieto di diffusione di qualsiasi informazione (acceduta direttamente o indirettamente).

[11] Per approfondimenti si veda "IT Control Objectives for Sarbanes Oxley – 2" ed. Appendix L

Non sempre il contratto di outsourcing contiene, o può contenere, clausole atte a regolamentare esplicitamente lo svolgimento di un Audit richiesto dal cliente. Non solo per ciò che concerne il diritto del cliente a richiederlo, ma anche alla descrizione dei processi da attivare e delle procedure da seguire, da parte di tutte le parti interessate, nel caso in cui tale diritto sia esercitato. Queste clausole, spesso richiamate come "Audit provisions" servono a tutelare entrambe le parti in quanto garantiscono l'ottimizzazione delle onerose fasi preliminari di accordo sui tempi, sui ruoli, sulle responsabilità, sui protocolli secondo i quali l'audit si svolgerà e sulle modalità di produzione dei piani di correzione delle carenze riscontrate; inoltre, (magari assicurando al cliente che lo "User Audit" verrà supportato nel più efficiente dei modi nel sito dell'outsourcer), queste clausole garantiscono anche all'outsourcer che la delicata fase del lavoro si svolgerà seguendo modalità concordate e soprattutto tali da minimizzare l'impatto sull'erogazione del servizio.

3.4 End Users Computing

Il contesto degli End Users Computing (EUC nel seguito) è stato uno degli ambiti in cui progressivamente, in un processo di disegno ed attuazione dei controlli interni a supporto dell'informativa finanziaria, si è focalizzata l'attenzione delle diverse società e degli "addetti ai lavori"; a motivo della constatata importanza e rischiosità implicita in tali applicazioni.

3.4.1 Definizione e caratteristiche

Il termine EUC individua un insieme di strumenti promossi, realizzati ed utilizzati direttamente dagli utenti finali al fine di ottenere maggiore efficienza su aspetti operativi e/o di controllo altrimenti demandati a manualità.
Le caratteristiche peculiari di tali strumenti di calcolo sono:

- coincidenza tra lo sviluppatore e l'utilizzatore finale;
- maggiore suscettibilità agli errori;
- possibilità di effettuare trattamento di dati in modo non formalizzato;
- controllo logico degli accessi poco strutturato o assente;
- bassa ripercorribilità degli sviluppi evolutivi o manutentivi effettuati;
- scarso livello di documentazione.

Alcuni esempi di prodotti / strumenti di sviluppo di End User Computing sono:

- fogli elettronici (ad es.: MS Excel);
- database manager (ad es.: MS Access, Oracle DB, Lotus Domino);
- query o script eseguiti direttamente sui database dagli utenti finali. (Ad es.: MYSQL, SQL Server, Power Builder, Easy Writer, Idea)

3.4.2 Linee guida sullo sviluppo dell'EUC e titolarità in azienda

La maggiore difficoltà nell'impostare e mantenere un modello di controllo sui prodotti EUC deriva dal fatto che qualunque utente più o meno esperto, assegnatario di una postazione di lavoro può realizzare applicazioni di questa natura, con livelli di complessità variegate.

Ulteriore elemento di complessità in questo contesto deriva dal fatto che gli sviluppi EUC, proprio perché realizzabili a livello individuale, vengono considerati come tali dagli stessi utenti, cioè strumenti ad uso e consumo individuale anziché componenti (fasi, attività, elaborati, input, output, etc.) di processi aziendali.

In questo contesto gli elementi da promuovere a cura del Dirigente Preposto (o dalle proprie strutture di supporto) in un contesto di controllo interno ai fini dell'informativa contabile e di bilancio sono:

- *linee guida sullo sviluppo*: dovrebbero essere promosse, con cadenza periodica da definirsi (ad es. semestrale) delle sessioni di censimento dei prodotti EUC attualmente in uso. Tale attività dovrebbe verosimilmente concentrarsi sulle strutture/funzioni che si qualificano come contributori (in qualunque misura) di processi in perimetro. La finalità ultima di questa fase è avere consapevolezza sulla numerosità e collocazione di applicazioni EUC.
- *titolarità*: dovrebbero essere progressivamente attribuite titolarità e ownership di tali strumenti. Sono da valutare, in funzione del contesto societario in cui si opera, soluzioni di titolarità in capo ad "owner" di controlli già individuati nelle fasi di impianto oppure (contestualmente al passaggio di consegne del prodotto EUC stesso o di parte di esso) anche ad altre funzioni aziendali. Finalità cardine di questa fase è l'identificazione dei vari attori nell'ambito dello EUC per l'attribuzione delle relative responsabilità.

Nei paragrafi che seguono, ipotizzato che a questo livello siano noti il numero e distribuzione degli EUC e la relativa titolarità, vengono proposti criteri di classificazione utili al disegno e messa in opera di un set di controlli minimali.

3.4.3 Criteri utili all'identificazione del perimetro di applicazioni EUC rilevanti per il Financial Reporting

Come già sottolineato, le applicazioni EUC hanno assunto notevole rilevanza all'interno dei processi aziendali, in quanto spesso direttamente impattanti sui dati di informativa contabile e di bilancio. Si rendono pertanto necessarie valutazioni circa l'integrità dei dati in esse contenuti ed elaborati.

La rilevanza dell'integrità dei dati contenuti negli EUC è principalmente basata - se non direttamente proporzionale - al loro utilizzo (finanziario, gestionale, operativo) e sull'analisi del rischio ad essi attribuibile.

Nel determinare quali EUC siano rilevanti per l'informativa contabile e di bilancio, i passi logici da compiere sono:

- associazione dell'EUC ai processi in perimetro;
- valutazione della rilevanza (materialità) dei dati trattati dall'EUC;
- valutazione della complessità dell'EUC.

3.4.3.1 Associazione dell'EUC a processi in perimetro

Gli EUC che devono essere valutati secondo i due modelli che seguono, devono essere generati ed essere di supporto ai processi amministrativo/contabili classificati in "scopo" per l'informativa finanziaria.

3.4.3.2 Valutazione della rilevanza (materialità) dei dati trattati dall'EUC

La rilevanza degli EUC può essere valutata sulla base delle informazioni in essi contenute, e in base alle quali possono essere suddivisi nelle seguenti categorie ad importanza progressivamente crescente:

- Operativi: consentono la tracciabilità e il monitoraggio del flusso di lavoro a supporto dei processi operativi (ad es. lista dei reclami aperti, fatture non pagate o qualsiasi altra informazione che precedentemente sarebbe stata gestita in modo manuale e archiviata in maniera cartacea). A tal fine i fogli possono essere usati per monitorare e controllare che le transazioni finanziarie siano catturate in maniera appropriata e completa.
- Gestionali: utilizzati per supportare la verifica analitica delle informazioni e il processo decisionale del management. A tal fine i fogli possono essere usati per valutare la ragionevolezza degli importi.
- Di bilancio: utilizzati per il calcolo degli importi delle transazioni o i saldi di bilancio. Tali informazioni sono inserite in contabilità generale e/o in bilancio.

Premesso che tutte e tre le tipologie possono essere rilevanti ed, in genere, in ordine crescente di importanza, un altro passo di valutazione è da ricercarsi nella significatività/rilevanza dei dati generati e/o gestiti da tali applicazioni. In questo contesto il termine più comunemente utilizzato è quello di materialità, che denota una soglia economica superata la quale il prodotto EUC è da considerarsi incluso nell'ambito di progetto e come tale dovranno essere disegnati controlli su di esso.

3.4.3.3Valutazione della complessità dell'EUC

Gli EUC possono avere differente complessità, in genere identificabile con i seguenti attributi qualitativi:

- Bassa: utilizzati come strumento per tracciare alcune informazioni comunque disponibili e leggibili da altra fonte.
- Moderata: utilizzati per svolgere calcoli semplici come l'uso di formule per totalizzare alcuni campi o moltiplicare dei valori. In questo modo i fogli sono utilizzati come metodo per tradurre o formattare delle informazioni, utilizzati come "Decision support systems (DSS)" oppure per registrare le entrate nel libro giornale o per preparare l'informativa societaria;
- Alta: oltre agli scopi del punto precedente, sono caratterizzate da calcoli complessi, dall'uso di macro o da fogli multipli dove celle, valori e fogli individuali sono collegati tra loro. Questi possono essere considerati applicativi veri e propri.

Si riportano di seguito alcune caratteristiche da considerare nel valutare la complessità di un foglio di lavoro o di un EUC:

1. sensibilità all' errore (ad es. l'ingresso di errore o errore logico);
2. metodo di creazione (ad es. estrazioni automatiche, creazioni manuali);
3. utilizzo di macro e fogli di lavoro collegati/database;
4. utilizzo di riferimenti complessi, calcoli e tabelle pivot;
5. numero di query, report e relazioni utilizzati;
6. numero di indici, campi, dati, colonne e righe utilizzate;
7. numero di utilizzatori;
8. rilevanza dell'output;
9. frequenza e portata dei cambiamenti e delle modifiche al foglio di lavoro.

Tanto più numerose sono le caratteristiche dell'EUC in esame, tanto maggiore sarà la sua complessità.

3.4.4 Formulazione di criteri per l'individuazione di un set minimale di controlli ITGC

Per valutare la tipologia ed il grado dei controlli che dovrebbero essere applicati, sono anzitutto da individuare un set di obiettivi di controllo minimale le cui implementazioni sono ancora funzione delle valutazione di rilevanza e complessità prima citate.
Il tutto, come anzidetto, per EUC individuate all'interno di processi contabili e di bilancio (Financial Reporting Processes).

Sono di seguito elencati gli obiettivi di controllo pertinenti per valutare l'applicazione (disegno ed operatività) dei controlli di I° livello istituiti in funzione della natura e complessità degli EUC.

Obiettivi di controllo:

- CHANGE CONTROL: gestire un processo per le richieste di cambiamento, apportare i cambiamenti, testare il contenuto del foglio a garanzia che il cambiamento sia stato fatto in coerenza con le aspettative;
  VERSION CONTROL: assicurare che le versioni utilizzate siano correnti e approvate. Questo può essere assicurato utilizzando delle regole di codifica standard (nome del documento); rivedere la logica utilizzata per creare e gestire il foglio di calcolo e documentare lo svolgimento dell'attività;
- ACCESS CONTROL: salvare i documenti in una cartella con accesso limitato alle sole persone autorizzate e/o proteggere il file con password per limitarne l'accesso;
- INPUT CONTROL: assicurare un processo di riconciliazione per garantire che i dati siano stati correttamente e accuratamente inseriti. I dati possono essere inseriti manualmente o in modo sistematico attraverso download. La riconciliazione dei dati di input deve essere effettuata/tracciata attraverso il confronto tra le fonti dei dati di input e i dati inseriti nel foglio di calcolo ovvero si può rimandare all'esecuzione di un controllo chiave qualora tale controllo garantisca anche la correttezza dei dati di input;
- SECURITY AND INTEGRITY OF DATA: implementare un processo per assicurare che i dati inclusi nei fogli siano corretti e integri. Questo può essere fatto bloccando o proteggendo le celle per prevenire cambiamenti involontari e/o intenzionali ai dati standard;
- DOCUMENTATION: assicurare che le modalità di utilizzo del foglio di calcolo siano documentate in modo appropriato e aggiornate per capire l'obiettivo di business e le specifiche funzioni del foglio. Le informazioni possono essere raccolte attraverso la compilazione/aggiornamento di un foglio di "documentation" inserito nel file di calcolo. Tale foglio di "documentation" può essere utilizzato anche per tracciare l'effettuazione di altri controlli (ad es. a - change control, d - input control etc.);
- DEVELOPMENT LIFECYCLE: applicare la normativa del ciclo di vita di sviluppo software per il processo di sviluppo degli EUC di complessità Alta. Il processo dovrebbe includere le specifiche tecniche, la progettazione, la costruzione, il collaudo e la manutenzione. Il collaudo è un controllo critico per garantire che il foglio di lavoro produca risultati accurati e completi;
- BACKUP e ARCHIVING: assicurare un processo di backup periodico per i fogli di calcolo per garantire la disponibilità completa ed accurata delle informazioni ai fini del financial reporting; archiviare i file non più suscettibili di cambiamenti in una cartella separata e salvare i documenti in sola lettura o in formato PDF;
- SEGREGATION OF DUTIES/ROLES AND PROCEDURES: verificare sulla base dei controlli applicabili (si vedano i controlli precedenti) che le seguenti segregazioni di ruoli e responsabilità siano assicurate:
  - la persona che effettua il cambiamento deve essere diversa dalla persona che ne verifica/collauda l'effettuazione (si veda Change Control);
  - la persona che effettua l'imputazione dei dati deve essere diversa dalla persona che effettua la riconciliazione tra i dati di input e le fonti dei dati (si veda Input Control);
  - la persona che effettua la "logic inspection" deve essere diversa dalla persona che ha sviluppato o che utilizza il foglio di calcolo (si veda Version Control).

Natura e complessità degli EUC: proposte di implementazione

Il livello dei controlli da implementare dovrebbe essere individuato dal Management in base all'utilizzo del foglio di lavoro, alla complessità ed all'affidabilità richiesta dell'informazione.

Si riporta nella tabella sottostante il set di controlli che, secondo le linee guida qui espresse, dovrebbe essere garantito sugli EUC in base alla loro tipologia e complessità.

Controlli	Tipologia e complessità	Contabile e bilancio			Gestionale			Operativo		
		High	Moderate	Low	High	Moderate	Low	High	Moderate	Low
a) Change Control		X								
b) Version Control		X	X	X	X	X				
c) Access Control		X	X	X	X	X		X		
d) Input Control		X	X	X	X	X	X	X	X	
e) Security & Integrity		X			X					
f) Documentation		X			X					
g) Development lifecycle		X								
h) Back-Up		X	X	X	X	X	X	X	X	
i) Segregation of Duties		X	X							

Tab. 4

La lettura della tabella di sintesi suggerisce l'implementazione di tutti gli obiettivi di controllo elencati in presenza di un EUC di natura contabile e di bilancio, complessità alta e materialità superiore alla soglia predefinita. Dal lato opposto un EUC di natura operativa, complessità bassa seppure materiale potrebbe addirittura non richiede l'implementazione di alcun controllo.

3.5 Riferimenti bibliografici

- **COBIT® 4.1**
  IT Governance Institute, maggio 2007

- **IT Control Objectives for Sarbanes-Oxley**
  The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition - IT Governance Institute, settembre 2006
  (Edizione in lingua italiana: settembre 2008, a cura di ISACA Roma)

- **Internal Control - Integrated Framework**
  By the Committee Of Sponsoring Organizations of the Treadway Commission (COSO) (1992)

- **Enterprise Risk Management – Integrated Framework**
  By the Committee Of Sponsoring Organizations of the Treadway Commission (COSO) (settembre 2004)

- **PCAOB Audit Standard No. 5 – luglio 2007**

- **Information Technology Infrastructure Library v3 (ITIL v3)**
  OGC, 2005

4 APPLICATION CONTROLS, SEGREGATION OF DUTIES, OBIETTIVI/RISCHI PER SETTORE INDUSTRIALE

(FOCUS GROUP 4)

Introduzione

Obiettivo dei tre Capitoli seguenti è di fornire uno schema di governo per ognuno dei tre contesti (Controlli Applicativi, Segregazione dei compiti, e Obiettivi/Rischi) che risulti coerente con il modello COBIT®.

4.1 Controlli applicativi

Un sistema applicativo può essere definito come un prodotto software che permette ad un utente di svolgere delle attività utilizzando le capacità elaborative di un computer. In generale, i sistemi applicativi possono essere classificati in: sistemi che trattano applicazioni transazionali e sistemi che trattano applicazioni di supporto. Nella prima tipologia rientrano le applicazioni che elaborano dati e registrano valori contabili (ad esempio: crediti e debiti), costituiscono archivi di dati finanziari e operativi, permettono il reporting finanziario/contabile. Ad esempio possiamo citare SAP R/3, Oracle Financials, Peoplesoft, ACG. Nella seconda categoria rientrano invece i sistemi applicativi che facilitano le attività aziendali, quali posta elettronica, trattamento immagini, progettazione, etc., e non elaborano quindi dati contabili.

L'utilizzo di sistemi applicativi transazionali espone l'azienda a rischi di integrità, completezza, tempestività e disponibilità dei dati contabili/finanziari; pertanto, è necessario definire dei controlli all'interno di tali sistemi, atti a mitigare tali rischi.

Come descritto da COBIT® for SOX[12] i controlli applicativi sui processi di business si articolano in controlli manuali, controlli automatici e controlli ibridi (controlli manuali dipendenti da procedure IT).[13]

[12] IT Control Objectives for SOX, App. D:

1. Controlli automatizzati – sviluppati nell'ambito dei sistemi applicativi secondo una logica binaria, operano come sono stati progettati e di norma meno soggetti ad errori, rispetto a quelli manuali. Esempi di tali controlli sono:
   a. Attività di quadratura (controllo sui saldi - *balancing control*) – controlli che intercettano gli errori nel *data entry* per mezzo della riconciliazione dei valori inseriti manualmente o in automatico in un totale di controllo.
   b. *Check digit* – validazione dei dati attraverso un procedimento di calcolo.
   c. Liste di dati predefinite – controlli che forniscono all'utilizzatore liste predefinite di dati che possono essere accettati.
   d. Test di ragionevolezza sui dati – test che confrontano i dati catturati rispetto un *pattern* costante o di ragionevolezza.
   e. Test logici – test che includono l'uso di limiti di *range* o test di valore / alfanumerico.
   f. (Ri) calcoli – calcoli numerici sviluppati da routine interne nelle applicazioni.

Per la nozione di controllo automatico si adottano le seguenti regole e interpretazioni:

Nell'ambito di una procedura automatizzata si distingue tra processo principale e processo di controllo (in breve controllo).

Ad esempio il calcolo del totale per riga fattura (quantità per prezzo) e relativa IVA sono un processo principale automatico della procedura di fatturazione; tale processo sarà assistito da controlli automatici che verificano che il nome cliente, il codice prodotto e relativo prezzo e aliquota IVA siano ammissibili.

Nonostante l'automatismo, nessun controllo può essere dato per esistente se non ne viene puntualmente accertata l'operatività.

In termini formali, intendendosi per operazione (in inglese tipicamente "transaction") un'attività richiesta da un utente o da un programma, un controllo è automatico quando la sua esecuzione è provocata dall'input dell'operazione o da altra condizione dipendente dall'operazione non alterabile dall'utente senza evidenza, e si svolge secondo una delle seguenti modalità:

1. Verifica l'ammissibilità del tipo di operazione sulla base di una tabella di autorizzazione (tipo evento, soggetti, condizioni.
2. Verifica l'ammissibilità dell'operazione sulla base di algoritmi che controllino la ragionevolezza di uno o più campi numerici descrittivi dell'evento (numbers, dates, time, percent, etc).
3. Fornisce chiara evidenza (data e ora) dell'avvenuto controllo e del dispositivo (hw o sw) che lo ha effettuato.

Sono <u>controlli applicativi automatici di I° livello</u>:

1. Ammissibilità / autorizzazione di:
    - Causali (descrivono il tipo di evento).
    - Date / ore.
    - Sintassi di un campo.
    - Nomi, codifiche o parole chiave.
    - Importi.
    - Ruoli e responsabilità (Segregation of duties).

2. Controlli IT dipendenti da azioni manuali (detti controlli ibridi): si tratta essenzialmente di controlli manuali che dipendono dai sistemi IT. Esempi di tali controlli sono i report generati a richiesta dai sistemi applicativi. (sono usati per fornire dati per il management review).

[13] In passato una classificazione di controlli basata sulla sequenza logica e temporale di un processo principale prevedeva i controlli di input, di processing e di output. Tali nozioni si ritengono superate dal principio del rischio come guida ai controlli e dell'incerto confine tra controllo di input, processing e output.

Sono controlli di supervisione sui suddetti controlli di I° livello:

1. La consultazione e "follow-on" scritto/registrato per tutte le eccezioni riportate da tali controlli, siano essi:
   - Esiti con eccezioni di eventi registrati.
   - Esiti con warning e conferma di eventi registrati.
   - Lista degli eventi respinti (in stato di sospensione).
   - Lista delle date ed eventi associati a periodi o situazioni in cui i controlli di I° livello sono stati sospesi o alterati.

Sono controlli di 3° livello (verifiche di Audit):

1. L'estrazione e la valutazione rispetto all'obiettivo di controllo delle tabelle, algoritmi e maschere di autorizzazione, persone autorizzate alle modifiche di tali tabelle.
2. La consultazione di un campione significativo di eventi registrati per la verifica di accuratezza e completezza delle liste di eccezioni (ricerca di valori di eccezione, loro puntuale riporto nelle liste eccezioni).
3. La consultazione per una localizzazione e periodo delle liste eccezioni per valutare le azioni di follow-on adottate dal supervisore.

L'estrema numerosità dei campi da verificare richiede all'auditor di applicare una rigorosa tecnica di risk assessment per limitare il numero di verifiche dei suddetti controlli.

L'adozione di una procedura di fatturazione supportata da un prodotto commerciale noto e stimato nulla dice sulla esecuzione dei controlli, ma può essere un valido argomento, in sede di risk assessment della procedura, per esprimere una misura ridotta di rischio per le finalità di Audit.

Un controllo è ibrido quando esso è svolto da un operatore sulla base di un elaborato IT, a sua volta non oggetto di specifica verifica alternativa. La produzione dell'elaborato inoltre può essere subordinata ad una iniziativa di un utente (o controllore).

L'attendibilità dell'elaborato rientra nelle verifiche di correttezza dello sviluppo del software applicativo; l'audit dovrà aggiungere ai controlli 1, 2 e 3 sopraddetti, una analisi delle evidenze che permettano di valutare se il controllo è stato effettivamente eseguito per tutti gli eventi per i quali esso era previsto.

Controlli ibridi e controlli automatici sono la maggioranza dei controlli applicativi.

Controlli manuali di 1° livello sono tipicamente:

- Conta fisica di modulistica in bianco (per procedure IT)
- Riconciliazione (analisi delle componenti di una riconciliazione)

Controlli manuali di 2° livello sono tipicamente:

- Controlli di supervisione che prevedono una seconda lettura di elaborati.
- Firme di autorizzazione.

L'Audit dei controlli manuali anzidetti si fonda sulla rilettura a campione delle evidenze dei controlli di 1° e di 2° livello.

I controlli automatizzati devono essere quindi inseriti *(embedded)* all'interno del Software applicativo per prevenire o intercettare le transazioni non autorizzate e garantire la completezza, l'accuratezza e la corretta elaborazione delle transazioni.
A differenza dei controlli generali, i controlli applicativi sono connessi alle transazioni ed ai dati pertinenti a ciascun sistema applicativo. L'obiettivo dei controlli applicativi è di garantire la completezza e accuratezza delle registrazioni, nonché la validità delle modifiche apportate ai dati in seguito all'elaborazione dei programmi e sono quindi specifici per ciascuno di essi (rif. *ISACA, IS Auditing Guideline – Application Systems Review, Document G14*, p. 3).

Le aziende che non considerano opportunamente i controlli applicativi quando valutano o certificano il proprio sistema dei controlli interni, possono incorrere nel rischio di non raggiungere la conformità alla normativa.

Molto frequentemente le aziende assumono che i loro sistemi di *financial reporting* siano affidabili perché non hanno mai riscontrato problemi oppure perché ritengono di aver testato adeguatamente il software o perché si affidano ai controlli manuali; in tale modo, tuttavia, non vengono valutati i rischi che potenziali insiti in un sistema applicativo. Tutto ciò può portare a sottostimare debolezze materiali nel controllo interno.

In generale le aziende caratterizzate da sistemi informativi complessi stanno rivedendo le loro applicazioni più rilevanti per analizzare come esse siano di supporto al processo di *financial reporting.* A tal fine vengono documentati i controllo sull'integrità delle applicazioni mediante l'analisi e il collaudo dei controlli rilevanti implementati nelle applicazioni finanziarie al fine di confermare il disegno e l'efficacia (processo di *benchmarking).*

Relazione tra controlli applicativi e ITGC

I controlli generali IT, che hanno anch'essi il fine di garantire l'affidabilità delle informazioni contabili e di bilancio aziendali, supportano il funzionamento dei controlli applicativi; entrambi sono necessari per garantire un *processing* accurato e l'integrità delle informazioni utilizzate per governare e produrre i report aziendali. Tali controlli si applicano a tutti i sistemi, processi e dati presenti in un'organizzazione o un sistema informativo (rif. *GTAG 1: Information Technology Controls*, p. 3).

La relazione tra i controlli applicativi ed i controlli generali IT può essere sintetizzata come segue: i controlli generali IT sono necessari per garantire l'affidabilità (*reliability*) dei controlli applicativi automatici e ibridi. Sebbene criticità sui controlli generali IT non producano direttamente errori nelle scritture contabili (*financial statement*), un'applicazione IT che poggi su infrastrutture i cui controlli generali siano inefficaci è esposta al rischio di alterazione di funzionalità o di interruzione della propria operatività, al rischio di alterazione dei propri processi autorizzativi e delle proprie basi dati. Quindi la significatività dei controlli IT generali deve essere valutata in relazione ai suoi effetti sulla integrità dei dati trattati dagli applicativi, e sulla regolarità dei loro controlli.

Responsabilità dell'implementazione

È opportuno che i responsabili per i controlli applicativi specifici dei processi di *business* siano i relativi *business owner*. È responsabilità della funzione IT assistere i b*usiness owner* nell'identificazione e test di tali controlli e contemporaneamente assicurare che i controlli applicativi generali (restrizioni all'accesso, *change control, backup recovery* ecc.) esistano e siano affidabili.

In sintesi quindi è responsabilità delle funzioni di business:

- definire i requisiti funzionali dei controlli applicativi mitiganti i rischi di integrità del financial reporting;
- utilizzare le evidenze prodotte dai controlli applicativi.

E' invece responsabilità della funzione sistemi informativi:

- implementare i controlli applicativi secondo le specifiche definite dalle funzioni di business;
- definire ed rendere effettivi i controlli generali IT (ITGC) a garanzia dell'integrità dei controlli applicativi.

Identificazione e valutazione dei controlli applicativi

Pianificazione e scoping delle attività sui controlli applicativi

I progetti rilevanti richiedono particolare attenzione alla fase di pianificazione delle attività e di individuazione del perimetro di intervento. Ciò è richiesto anche nell'analisi dei controlli applicativi in particolare nell'ambito dei progetti di compliance alla Legge 262/2005. Le aziende gestiscono numerosi processi di business con i relativi controlli, ma gli obiettivi di integrità del financial reporting, richiedono la selezione di quei processi e controlli che sono di supporto alla generazione del financial reporting. Di conseguenza, è importante che il team di IT Compliance partecipi all'identificazione dei controlli applicativi. Al riguardo di norma esistono due possibili approcci:

- il team dei controlli IT partecipa con il team dei controlli contabili e di business all'identificazione dei controlli applicativi;
- il team dei controlli finanziari e di business identifica prima tutti i controlli e poi il team dei controlli IT li rivede per identificare quali sono dipendenti dall'IT.

Considerazioni sulla selezione dei controlli applicativi (risk based approach)

L'applicazione pratica di quanto sopra descritto richiede alcune considerazioni sulle modalità di scelta dei controlli applicativi e dei criteri che debbono ispirare questa delicata fase. Una corretta attività di selezione degli application controls permette di ottenere i seguenti vantaggi:

- riduzione dell'ambito di analisi e testing dei controlli;
- individuazione dei controlli effettivamente in grado di mitigare i rischi;
- efficienza nell'ottenimento della compliance.

In primis occorre effettuare una mappatura delle applicazioni rilevanti ai fini della reportistica finanziaria. Tale mappatura permette di individuare, e quindi limitare l'ambito di analisi alle applicazioni che supportano i processi di alimentazione delle voci di bilancio rilevanti.

E' bene in tale fase raccogliere informazioni relative al contesto tecnologico ove le applicazioni sono inserite. A titolo esemplificativo vanno raccolte le informazioni relative a linguaggio di programmazione, DBMS utilizzato, piattaforma hardware e relativo sistema operativo ove l'applicazione è installata, etc.

Censite le applicazioni rilevanti per il financial reporting, occorrerà procedere alla identificazione dei controlli sulle applicazioni che sono dipendenti dall'IT e per ciascuno di essi individuare il relativo responsabile. L'individuazione del responsabile del controllo richiede particolare attenzione in quanto la responsabilità relativa ai controlli applicativi è nella maggior parte dei casi condivisa tra IT e funzioni di business.

L'individuazione dei controlli applicativi dovrà essere quanto più possibile limitato ai controlli a garanzia dell'integrità del financial reporting, adottando un approccio basato sul rischio (Risk Based Approach). Questo richiede l'individuazione del rischio inerente[14] e del rischio residuo (ciò che residua dopo l'applicazione dei controlli) e si basa su considerazioni legate alla probabilità del verificarsi dell'evento rischioso e considerazioni legate all'impatto.

---

[14] Il rischio di audit si può suddividere nelle seguenti categorie:

Rischio inerente - Il rischio che esista un errore che può diventare materiale o significativo quando esso è combinato con altri errori riscontrati durante l'audit, presumendo che non ci siano controlli compensativi. Il rischio inerente si può anche esprimere come la possibilità che si verifichi un errore materiale in assenza dei relativi controlli. Per esempio: è più probabile che si commettano errori nei calcoli complessi che in quelli semplici; oppure il denaro contante ha più probabilità di essere rubato di uno stock di carbone. Il rischio inerente esiste indipendentemente dall'audit e può essere conseguenza della natura del business.

Rischio di controllo - Il rischio di controllo che un errore materiale esista ma non venga prevenuto o riscontato tempestivamente dal sistema dei controlli interni. Ad esempio, il rischio di controllo associato alla verifica manuale di log di computer può essere alto in quanto condizioni che richiedono ulteriori chiarimenti passano di frequente inosservate a causa del volume di informazioni raccolte nel log. Il rischio di controllo associato a procedure automatizzate di validazione dei dati è normalmente ridotto perchè questo processo è svolto con sistematicità.

Rischio d'indagine (detention risk) - Il rischio che un auditor si Sistemi Informativi usi procedure di verifica adeguate e pervenga alla conclusione che non esistono errori materiali quando, in effetti, questi si sono verificati. Un errore non verrebbe individuato durante la fase di valutazione del rischio di un audit. L'identificazione del rischio di indagine consentirebbe però una valutazione più favorevole della capacità dell'auditor di identificare e correggere errori materiali a seguito di un'attività di test.

Rischio complessivo dell'audit - Il rischio complessivo dell'audit è la combinazione delle categorie individuali di rischi di audit valutati per ciascun obiettivo di controllo specifico. Un obiettivo di cui tenere conto nel formulare l'approccio di audit è quello di limitare il rischio di audit per l'area in esame così che il rischio complessivo di audit sia ad un livello sufficientemente basso al termine dell'indagine. Un altro obiettivo consiste nel valutare e controllare quei rischi per acquisire il livello desiderato di ragionevole certezza il più efficiente possibile.

Fonte: Manuale CISA 2009 - Capitolo 1, par. 1.6.6. Rischio di audit e materialità - ISACA (traduzione a cura di AIEA)

Tra i fattori che dovranno essere tenuti in considerazione nello svolgimento del risk assessment, possono essere ricompresi:

- natura della tecnologia (complessa o semplice);
- risorse umane coinvolte (con esperienza o senza esperienza);
- tipo di applicazione (package, personalizzata, sviluppata in house, ecc.);
- natura dei processi di business supportati dall'applicazione (critici/non critici);
- tipologia di dati trattati (riservati/non riservati);
- rilevanza del controllo (Key/Non key);
- frequenza dei cambiamenti all'applicazione o ai dati e complessità dei cambiamenti;
- esperienze passate.

Uno dei vantaggi correlati ad un approccio Risk Based consiste nella individuazione della natura e dell'estensione dei controlli da valutare e sottoporre a test. A titolo esemplificativo, se un'applicazione ha al proprio interno un numero molto limitato di controlli applicativi automatici e ibridi, allora è possibile escludere la verifica di tali controlli (e quindi dell'applicazione stessa) dall'ambito del progetto. In alternativa, si può identificare un controllo suppletivo di tipo manuale che sia rilevante oppure aumentare il grado di fiducia *(reliance) r*iposto sui controlli manuali già esistenti. Il grado di fiducia è una espressione soggettiva riguarda l'efficacia attesa da un controllo. Si tratta quindi del complemento del rischio di controllo.

Documentazione dei controlli

All'identificazione dei controlli deve seguire la loro documentazione, in modo da illustrare le modalità con le quali sono stati indirizzati i rischi circa il reporting non affidabile e mettere quindi il management in condizione di valutare la gestione del relativo rischio residuo.

Spesso i controlli applicativi sono inclusi nella documentazione del processo di *business*. Di solito gli specialisti IT documentano un processo in collaborazione con un esperto in materia di controlli ed insieme identificano le verifiche rilevanti per il processo. In molti casi la documentazione va rivista per identificare i controlli applicativi.

Solitamente la documentazione dei controlli applicativi può avvenire contestualmente alla rilevazione dell'intero sistema dei controlli per un processo, mediante flowchart e/o in forma descrittiva (*narrative*). La descrizione dei controlli dovrebbe prevedere:

- rischi identificati
- obiettivi di controllo
- attività di controllo
- attributi del controllo, quali tipologia (p.e. controllo preventivo, successivo) e frequenza del controllo (giornaliera, settimanale, mensile, etc.)
- informazioni per il test del controllo.

Valutazione disegno e test dei controlli applicativi

Completata la documentazione dei controlli applicativi, occorre valutare il disegno ed effettuare i test di operatività (o effettività). Tali attività dovranno essere descritte all'interno di un memorandum relativo alla pianificazione del lavoro di valutazione dei controlli applicativi, contente, tra gli altri:

- la descrizione delle procedure di review;
- le tecniche utilizzate per lo svolgimento delle attività;
- le modalità di campionamento utilizzate (se applicabile);
- le tempistiche.

La valutazione del disegno ha l'obiettivo di definire se il controllo è appropriato a mitigare i rischi per i quali è stato definito. La valutazione dell'efficacia operativa ha invece l'obiettivo di verificare, tramite test specifici, se il controllo è effettivamente operativo. Possibili modalità per effettuare il test di operatività sono:

- analisi della configurazione del sistema;
- analisi delle evidenze dei test di accettazione utente;
- analisi e/o riesecuzione delle procedure di riconciliazione;
- analisi delle liste utenti;
- riesecuzione del controllo in ambiente di test.

4.2 Principi di segregazione dei compiti

4.2.1 Introduzione

Questo capitolo si propone di illustrare le principali linee guida per lo sviluppo di controlli finalizzati a garantire un'adeguata separazione dei compiti in ambiti dove alcune responsabilità sono tra loro non compatibili. Come viene riportato nel documento "*IT Control Objectives for SOX 2nd Edition"* nell'Appendix M, *"Una adeguata segregazione di compiti è un elemento importante per determinare se le attività di controllo di una azienda sono efficaci per il raggiungimento degli obiettivi del controllo interno. Il concetto di base sottointeso nel concetto di 'segregazione di compiti' è che nessun impiegato o gruppo dovrebbe potersi trovare in una situazione tale che gli sia permesso nascondere errori o compiere frodi nel corso normale delle proprie attività".*

La segregazione o separazione dei compiti è anche definita come "*un controllo di base che previene o individua errori ed irregolarità assegnando a persone diverse le responsabilità di iniziare transazioni, registrarle e proteggere beni"* (rif*. "Manuale CISA"* ISACA). E' pertanto un mezzo fondamentale per scoraggiare o prevenire frodi o atti illeciti.
I principi esposti nel seguito possono quindi essere utilizzati sia per verifiche inerenti l'organizzazione aziendale, sia riguardanti processi aziendali o specifiche applicazioni informatiche. Inoltre, essendo un principio generale, la segregazione dei compiti è applicabile sia a processi automatici che manuali, sia a processi aziendali IT, sia non IT (vedi Par 4.2.3).

4.2.2 Segregazione dei compiti e matrice delle attività non compatibili

Un utile strumento di controllo per identificare responsabilità che non dovrebbero essere riunite in un unico soggetto è la matrice delle attività non compatibili (si veda esempio la successiva Figura 1).

		PROCESSO #1				…						PROCESSO #N		
		Sottoprocesso #1	Sottoprocesso #2	…	Sottoprocesso #H		…					Sottoprocesso #1	…	Sottoprocesso #K
PROCESSO #1	Sottoprocesso #1	-	I		D							D		I
	Sottoprocesso #2	I	-		I							I		I
	…			-	D									
	Sottoprocesso #H	D	I	D	-							I		I
…						-								
	…						-							
								-						
									-					
										-				
											-			
PROCESSO #N	Sottoprocesso #1	D	I		I							-		D
	…												-	
	Sottoprocesso #K	I	I		I							D		-

Figura 1 – Esempio di matrice delle attività non compatibili

In pratica, per ogni processo aziendale, si evidenziano i sotto-processi (nelle colonne e nelle righe della matrice) e per ogni casella si identificano quelle attività che non possono essere svolte dalla stessa persona o funzione aziendale.
Ad esempio, chi è responsabile del sotto-processo #H (all'interno del processo #1) non può svolgere il sotto-processo #2 (all'interno del processo #N): questa situazione è evidenziata dalla lettera "**I**" all'interno della matrice.

E' possibile ricomprendere nella matrice anche quelle attività che, pur essendo incompatibili, possono essere svolte dalla stessa persona o funzione, con opportune deroghe: queste attività vengono evidenziate nella matrice con la lettera "D". I rischi introdotti da queste incompatibilità devono essere mitigati attraverso opportuni controlli compensativi (a tal proposito si rimanda al Par. 4.2.4.2). Per esempio, in aziende di piccole dimensioni, i processi IT sono governati da poche persone e pertanto non è possibile separare completamente i compiti; è pertanto necessario implementare misure di controllo compensative.

4.2.3 Processi aziendali

I processi aziendali che entrano a far parte della matrice sono quelli giudicati rilevanti ai fini del Financial Reporting. Ad esempio: Gestione di Magazzino, Vendite, Acquisti ed anche processi Information Technology.

4.2.3.1Scelta delle attività non compatibili

L'analisi della compatibilità dei compiti viene effettuata a valle di un censimento delle attività, in base a fattori come:

- il grado di rischio nell'allocare un'attività ad una sola persona;
- la sovrapposizione di operatività o di ruolo;
- la dimensione dell'azienda.

In particolare, il rischio su di una attività deve essere valutabile attraverso un modello che agevoli la stima degli impatti potenziali in caso di errori o frodi su quella determinata attività.

4.2.3.2Esempi di attività non compatibili in ambito IT

In ambito IT la segregazione dei compiti deve trovare applicazione sia con riferimento ai cosiddetti IT Services al cui presidio sono deputati i controlli IT Generali (Vedasi FG3) sia con riferimento ai Business Processi al cui presidio sono deputati i Controlli Applicativi. Le attività non compatibili (e che pertanto andrebbero separate) relative al primo gruppo sono di norma le seguenti:

- Utenza dei sistemi informativi;
- Data entry;
- Esercizio dei sistemi;
- Gestione della rete;
- Amministrazione dei sistemi;
- Sviluppo e manutenzione dei sistemi;
- Gestione del cambiamento;
- Amministrazione della sicurezza;
- Audit.

A titolo esemplificativo si riporta di seguito una possibile matrice di attività IT non compatibili (Figura 2).

	Controllo	Analista / sistemista	Programmatore	Help Desk e supporto	Utente finale	Data entry	Operatore	DB admin	Network admin	System admin	Security admin	Tape admin	Programmatore di SO	Controllo qualità
Controllo	-	I	I	I		I	I	I	I	I			I	
Analista / sistemista	I	-		I	I		I				I	I		
Programmatore	I		-	I	I	I	I	I	I	I	I	I	I	
Help Desk e supporto	I	I	I	-	I	I		I	I	I		I	I	
Utente finale		I	I	I	-		I	I	I			I	I	I
Data entry	I		I	I		-	I	I	I	I	I		I	
Operatore	I	I	I		I	I	-	I	I	I	I		I	
DB admin	I		I	I	I	I	I	-	I	I			I	
Network admin	I		I	I	I	I	I	I	-			I		
System admin	I		I	I		I	I	I		-		I		
Security admin		I	I			I	I				-	I	I	
Tape admin		I	I	I	I				I	I	I	-	I	
Programmatore di SO	I		I	I	I	I	I	I			I	I	-	I
Controllo qualità					I								I	-

Figura 2 – Esempio di matrice dei processi IT non compatibili (Fonte ISACA)

Le attività non compatibili relative al secondo gruppo (Business Process) sono certamente diverse in relazione ai diversi Business process; esse tuttavia possono essere raggruppate in base ai seguenti criteri:

1. Deve essere assicurata indipendenza tra coloro che definiscono le procedure (che includono le regole di autorizzazione, i limiti alla spesa, i limiti di negoziazione, etc.) in applicazione dei business objectives e coloro che devono applicare tali procedure.

2. Deve essere assicurata indipendenza tra coloro che autorizzano i soggetti ammessi alla contrattazione con l'azienda e coloro che danno esecuzione ai contratti (compravendita, stipula di rapporti di finanziamento, di polizza di assicurazione, etc.).

3. Deve essere assicurata la separazione tra chi emette l'ordine di acquisto/vendita, chi riceve/spedisce, chi registra l'incasso/pagamento (tale separazione è il presupposto su cui si basa l'efficacia del controllo cosiddetto *three-way match*).

4.2.4 Controlli sui criteri di separazione di attività incompatibili

4.2.4.1 Attività non compatibili senza deroghe ("I")

Queste tipologie di attività devono essere separate a livello di struttura organizzativa e devono essere adottati alcuni meccanismi di controllo dedicati. Ad esempio:

- autorizzazione delle transazioni: la responsabilità è attribuita agli utenti e devono essere eseguiti controlli periodici per individuare eventuali transazioni non autorizzate;
- custodia dei beni: deve essere individuato il proprietario dei dati con responsabilità di stabilire i livelli di autorizzazione per l'accesso ai dati;
- accesso ai dati: i controlli sono costituiti da una combinazione di sicurezza fisica ed informatica. In quest'ultimo ambito devono essere applicati gli standard in materia di separazione dei compiti e privilegi minimi;
- moduli di autorizzazione per fornire evidenza dell'approvazione dei privilegi di accesso ai dati. Questi dovrebbero essere riesaminati periodicamente.

4.2.4.2 Attività non compatibili con deroghe ("D"): controlli compensativi

In aziende di piccole dimensioni la struttura organizzativa non permette una puntuale separazione degli addetti. In tale caso il sistema di controllo dovrà certamente prevedere controlli compensativi. Ad esempio:

- tracce di audit - dovrebbero consentire di ricostruire il flusso effettivo di una transazione. Sono considerate un buon controllo compensativo in caso di non completa separazione dei ruoli;
- riconciliazioni – sebbene si tratti di un controllo in carico all'utente, può essere utile che alcune quadrature vengano eseguite da un gruppo di controllo a conferma della corretta esecuzione di transazioni / funzionalità critiche.
- revisione da parte dei supervisori.
- riesame indipendente (audit interno o anche esterno).

Con riferimento ai controlli sui servizi IT, in ogni caso è indispensabile che:

- gli ambienti IT di sviluppo, collaudo e produzione siano tra loro separati anche ricorrendo a terzi soggetti (outsourcing).
- ci sia un'assunzione consapevole del rischio, conseguente ad un'attività di analisi dello stesso;
- sia in essere un processo autorizzativo per l'assegnazione dei profili abilitativi.

Nella nozione di piccole aziende si annoverano le realtà che si avvalgano di non più di 15 addetti a tempo pieno (incluse le attività svolte da terzi o da outsourcer, calcolando in tale caso il tempo totale equivalente) per lo svolgimento dei servizi IT a supporto dei sistemi applicativi utilizzati in azienda.

4.3 Rinvio agli obiettivi e rischi per settore industriale

I controlli Generali IT sono analoghi tra i diversi settori produttivi, essendo gli stessi finalizzati a ridurre i medesimi rischi associati all'utilizzo di sistemi informatici.
Analogamente, confrontando i modelli di controllo in uso in alcuni contesti (TLC, Finance, Automotive) non si riscontrano significative differenze nei diversi settori industriali per i singoli obiettivi di controllo (primari o secondari) presidiati.

Il grado di dettaglio e di formalità dell'analisi dei rischi di sicurezza e dei relativi Controlli IT aumenta notevolmente per le aziende che sono espressione o gestiscono le infrastrutture critiche del Paese (che riguardano l'approvvigionamento dell'energia, le telecomunicazioni, il sistema internazionale dei pagamenti).

Differenze di rilievo nei processi e nei controlli si riscontrano per i sistemi applicativi, i quali sono fortemente dipendenti dal settore, nonché dallo specifico ambito d'esercizio delle applicazioni informatiche.

5 VALUTAZIONE DEL SISTEMA DI CONTROLLO, FLUSSI DI ATTESTAZIONE E COMPLIANCE

(FOCUS GROUP 6)

5.1 Modello di valutazione del sistema di controllo interno

5.1.1 Introduzione

Il modello di valutazione delle inadeguatezze del sistema di controllo interno ai fini dell'attestazione del Dirigente Preposto e per la componente dei controlli in ambito Information Technology, dovrebbe condurre in ultima analisi alla individuazione delle eventuali "categorie dei controlli" che potenzialmente possono avere un impatto significativo sulla reportistica finanziaria e che pertanto, se del caso, debbano essere riportate nel Documento di Attestazione (vedi anche Paragrafo 6.2).

L'insieme dei controlli Generali IT rientra nella categoria dei controlli di tipo "pervasivo", che possono impattare trasversalmente,diversi processi di business aziendali le cui deficienze non sono direttamente riconducibili alle poste di conto economico. Ne discende che la quasi totalità dei controlli IT non sono valutabili in termini economici , né riconducibili a categorie quantitative.

Per garantire un'agevole ed efficace lettura delle anomalie e delle eccezioni, nel modello dei controlli in ambito IT sarà necessario adottare un processo di aggregazione degli stessi in "categorie" aventi caratteristiche omogenee in termini natura e rischiosità.

Al fine di assicurare che i controlli:

- consentano il raggiungimento dell'obiettivo di controllo ad essi associato,
- siano effettivamente applicati,
- garantiscano tempestivamente l'individuazione di errori e frodi,

è necessario introdurre un sistema di valutazione che prenda in considerazione sia l'efficacia del disegno che l'operatività dei controlli.

Il sistema di valutazione deve quindi trattare le eventuali "inadeguatezze" sui controlli secondo un flusso che ne fornisca:

1. l'identificazione e la classificazione,
2. la valutazione,
3. la risoluzione.

5.1.2 Identificazione di una inadeguatezza su un controllo

L'inadeguatezza si può concretizzare nell'*assenza* o nella *mancata applicazione* di un controllo necessario al raggiungimento dell'obiettivo, oppure in una *carenza* di un controllo esistente. In quest'ultimo caso, il controllo non sempre garantisce il raggiungimento dell'obiettivo di controllo o, viceversa, la copertura di un obiettivo di controllo non viene realizzata dal controllo (o da un insieme di controlli).

Queste tre tipologie di inadeguatezza (assenza, mancata applicazione, carenza del controllo) possono essere identificate sia in fase di valutazione del disegno (o, ancor prima, nell'ambito dell'attività di mappatura dei controlli), sia in fase di verifica dell'operatività dei controlli.

Alcune inadeguatezze nei controlli, per la marginalità degli elementi mancanti o carenti, potranno essere escluse dal processo valutazione.

5.1.3 Valutazione di una inadeguatezza su un controllo

Una volta che l'inadeguatezza sul controllo è stata identificata, è necessario procedere alla valutazione della stessa in termini di rischio e potenziali impatti sulla reportistica finanziaria.

La valutazione della componente di rischio a fronte di un'inadeguatezza si fonda sull'analisi di due fattori:

1. La **probabilità** di accadimento dell'errore dovuto alla mancanza del controllo (La probabilità di accadimento può misurarsi ad esempio su tre differenti livelli utilizzando quale riferimento un periodo temporale medio di 2-3 anni in cui stimarne la verificabilità).

2. L'**impatto** causato dall'errore potenziale

E' opportuno quindi stabilire una matrice di correlazione Probabilità vs Impatto che permetta di identificare/valutare la gravità dell'inadeguatezza.

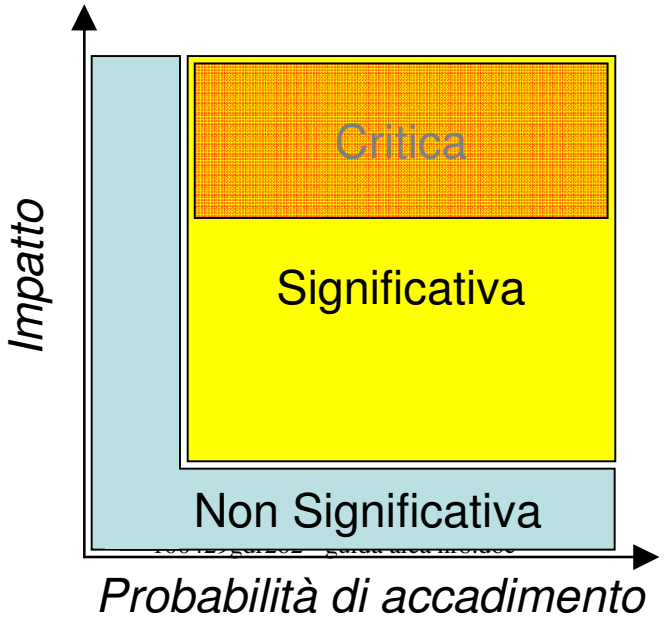


Figura 6.1 – Criticità delle inadeguatezze sui controlli

A seconda della probabilità di accadimento e della rilevanza dell'impatto, è possibile quindi classificare una inadeguatezza in:

- *Inadeguatezza Non Significativa*: è una inadeguatezza con basso impatto o con probabilità di accadimento bassa

- *Inadeguatezza Significativa*. E' possibile effettuare una ulteriore suddivisione in:
  - Inadeguatezza significativa *non-critica* cioè con impatto medio e probabilità di accadimento media.
  - Inadeguatezza *Critica* cioè con impatto alto o probabilità di accadimento medio-alta.

5.1.3.1 Criteri di valutazione dell'impatto e della probabilità di rischio

La valutazione della rilevanza dell' impatto e della probabilità di accadimento è basata sia su elementi quantitativi che su elementi qualitativi, come nel seguito illustrato.

Elementi quantitativi

Nel modello di valutazione si dovranno considerare e contribuiranno alla valutazione finale aspetti "quantitativi" quali:

- copertura dell'obiettivo di controllo associato al controllo;
- aggregazione delle inadeguatezze di controllo per "aree comuni", qualora esse siano correlate allo stesso processo o abbiano medesima natura. In questo caso le fasi di identificazione e valutazione vanno svolte sia a livello di singola inadeguatezza che a livello aggregato prendendo quindi in considerazione l'unione dei singoli impatti e delle singole probabilità di accadimento.

Uno schema di valutazione è proposto nell"*IT Control Objectives for Sarbanes-Oxley, 2nd Edition" (*Appendix I - Sample Deficiency Evaluation Decision Tree) attraverso uno schema decisionale guidato.

E' infine consigliabile effettuare la valutazione aggregata allo scopo di evidenziare eventuali inadeguatezze che singolarmente non sono critiche o significative *ma lo sono in aggregato.*

Elementi qualitativi

Nel modello di valutazione si dovranno considerare e contribuiranno alla valutazione finale aspetti quali:

- collegamento ai **controlli applicativi,** per cui si ritrova una chiara connessione tra la inadeguatezza del controllo Generale IT e un controllo Applicativo inefficace;
- **processi IT** in cui è stata rilevata l'inadeguatezza, quali ad esempio lo sviluppo software, la gestione delle Operations, la sicurezza fisica e logica, etc…;
- **pervasività (**impatto) sui diversi processi di business aziendali;
- **rilevanza** dell'**applicazione impattata**, in ragione, per esempio, del numero dei processi di business supportati;
- **"riferimento" al software applicativo**, in quanto ad esempio un controllo inefficace su una componente hardware è meno rilevante di un controllo inefficace sul change management del software applicativo;
- **"attinenza" con i sistemi contabili**, in quanto ad esempio un controllo inefficace su un'applicazione di "gestione della produzione" è meno rilevante di un controllo inefficace su un'applicazione "contabile";
- **storia degli errori** a fronte della inadeguatezza (ad esempio, limitazioni sui controlli del processo di sviluppo applicativo possono portare ad errori nelle elaborazioni dei dati di cui l'azienda può aver traccia nei sistemi di gestione degli incidenti ed anomalie, nell'IT Help-Desk od anche in altri dipartimenti IT).
- **numero di aziende** (nel caso di gruppo) impattate dalla inadeguatezza del controllo
- **persistenza dell'errore**, misurata attraverso il tempo di risoluzione dello stesso (breve, medio o lungo termine).

5.1.4 Risoluzione di una inadeguatezza su un controllo

La risoluzione dell'inadeguatezza su un controllo consiste nella definizione ed esecuzione di un "piano di azioni" (od anche piani di rimedio) e, a completamento del piano, nel successivo test di efficacia del controllo.

Il "piano di azioni" deve descrivere in modo accurato:

- il responsabile del piano;
- eventuali altre figure professionali coinvolte nell'attuazione del piano;
- le azioni correttive da implementare con le risorse necessarie;
- la scadenza del piano.

Il monitoraggio del "piano di azioni" deve verificare che gli aspetti dell'inadeguatezza riscontrati in fase di test siano stati progressivamente risolti. Il test di operatività del controllo, "a valle" del completamento del piano, chiude il processo di risoluzione dell'inadeguatezza.

Attraverso il modello di valutazione descritto, la gestione della inadeguatezza sul controllo con il relativo "piano di azioni" concorre al miglioramento del controllo stesso.

5.1.5 Considerazioni finali sul modello di valutazione

Chiave del modello di valutazione delle inadeguatezze rilevate nella fase di test è la metodologia adottata. E' quindi fondamentale tenere presente alcuni principi generali che permetteranno di valutare l'impatto e la probabilità di accadimento nel modo più aderente possibile alla realtà aziendale:

- Cambiamenti organizzativi possono "estendere" le debolezze evidenziate in un'area o business unit coinvolgendo quindi altri controlli.

- Lo stesso evento che ha causato l'inadeguatezza oggetto di valutazione può potenzialmente generare altre inadeguatezze.

Ulteriore elemento da considerare è la "gestione" di eventuali "Outsourcer", a cui è demandata interamente o parzialmente la gestione di alcuni processi IT.
La valutazione dei controlli "esternalizzati" (controlli la cui esecuzione è demandate a terzi ma la cui responsabilità ricade in capo all'azienda) dovrà essere assimilata e seguire il medesimo processo di valutazione in quanto l'eventuale inefficacia di un controllo "esternalizzato" (o la sua assenza) impatta in egual misura il sistema di controllo interno aziendale.

5.2 Flussi interni di attestazione

5.2.1 Introduzione

Nell'elencazione dei compiti attribuiti al dirigente preposto, il legislatore ha riassunto all'interno dell'art. 154-bis le varie funzioni ad esso spettanti. Il secondo comma della disposizione in esame stabilisce, in particolare, che gli atti e le comunicazioni della società diffusi al mercato e relativi all'informativa contabile anche infrannuale debbano essere accompagnati da una dichiarazione scritta del dirigente preposto, con la quale lo stesso attesti la corrispondenza alle risultanze documentali, ai libri e alle scritture contabili.

A tale riguardo il Position Paper ANDAF[15] sottolinea la maggiore complessità dell'attività di verifica dei controlli in essere da parte del DP nell'ambito di un Gruppo in quanto il DP dovrà attestare la corrispondenza di dati finanziari, riportati nel bilancio consolidato, prodotti da società controllate i cui processi amministrativo/contabili non sono, specialmente all'interno dei gruppi più complessi, direttamente sotto la sua supervisione.

[15] Position Paper ANDAF – Documento di consultazione "Il dirigente preposto alla redazione dei documenti contabili societari" Analisi, interpretazioni e proposte ANDAF Maggio 2007

L'approccio seguito da molti Gruppi di imprese americane ai fini della Sezione 404 del Sarbanes-Oxley Act del 2002, consiste nel creare un processo di "catena di attestazioni" mediante il quale le società controllate certificano l'adeguatezza del sistema di controllo internoai fini della formazione del bilancio che verrà successivamente consolidato dalla controllante.

Con tale approccio il processo di attestazione risulta essere più snello ed efficiente per i diversi attori, specialmente nel caso di grandi Gruppi.

5.2.2 Ipotesi di flusso di attestazione

E' quindi importante definire flussi interni di comunicazione tra l'IT e il Dirigente Preposto per consentire il corretto processo di valutazione del sistema di controllo interno nel suo complesso.

A tale riguardo possono essere definite modalità di comunicazione, in analogia con il processo a cascata precedentemente introdotto, per supportare il Dirigente Preposto nella sua attestazione.

Le modalità di comunicazione dovrebbero essere definite nell'ambito della struttura organizzativa o, inizialmente, nell'organizzazione del progetto, in modo da assicurare un processo congiunto (Finance, IT) di analisi e valutazione dei risultati dell'attività di test del disegno e dell'operatività dei controlli.

In ambito IT ed in organizzazioni complesse il flusso di comunicazione verso il DP potrebbe seguire due possibili modelli, schematizzati nella Tabella successiva:

Tipologia	Descrizione	PRO	CONTRO
Centralizzato	I risultati in ambito IT sono comunicati da ciascun CIO al DP responsabile dell'Internal Control over Financial Reporting.	Consente, a livello di holding, una più facile analisi in aggregato dei gap rilevati a livello di singola controllata.	Il processo congiunto (Finance ed IT) di valutazione delle inadeguatezze coinvolge solo i team Corporate.
Distribuito	I risultati in ambito IT vengono comunicati dal CIO della controllata al CFO/DP della stessa. Sarà poi compito dei CFO/DP delle controllate fornire al DP della holding i risultati.	Responsabilizzazione dei CFO delle società controllate sulle problematiche IT locali.	Potrebbe mancare, a livello di holding, un'analisi in aggregato dei gap rilevati a livello di singola controllata. Non è applicabile a processi IT - applicazioni gestite centralmente.

Tabella 6.1

A titolo di esempio si riportano di seguito alcuni modelli di comunicazione che il CIO potrebbe inviare al DP quale sintesi delle attività svolte e dei risultati ottenuti.

5.2.3 Esempi

ESEMPIO 1 - CERTIFICATION LETTER CIO

Con riferimento alle attività svolte per la valutazione sull'adeguatezza e l'effettiva applicazione, nell'esercizio ----, delle procedure di controllo sui sistemi informativi a supporto delle procedure amministrative e contabili e dei relativi controlli, Vi confermo quanto segue:

a) la documentazione in ambito ICT del Sistema di Controllo Interno sul Reporting Finanziario è rappresentativa delle procedure adottate;

b) tutti i controlli primari individuati per le applicazioni e le relative componenti tecnologiche in perimetro, per l'esercizio ----, sono stati testati per verificarne l'effettiva operatività e, in relazione alle risultanze, ove ritenuto opportuno, sono stati individuati i controlli compensativi e/o posti in essere adeguati piani di azione;

c) in allegato sono riportate le risultanze dell'attività di verifica dell'adeguatezza e dell'efficacia del Sistema di Controllo Interno sul Reporting Finanziario relative all'esercizio ----, in ambito ICT.

ESEMPIO 2 : *MODELLO DI ATTESTAZIONE DEL RESPONSABILE DI PROCESSO VERSO IL RESPONSABILE/CFO DI REPORTING UNIT/BUSINESS UNIT*

Io sottoscritto …
- nella mia qualità di responsabile, al 31.12.20xx, dei seguenti Processi:

  - …..

- tenuto conto delle risultanze documentate,

premesso

- che nel corso dell'anno 20xx e con riferimento alla chiusura contabile dell'esercizio 20xx le diverse fasi in cui i Processi si articolano sono state fatte oggetto di verifiche e controlli, e che in particolare:

  - risultano completate le attività di analisi e di test dei controlli;
  - tutte le inadeguatezze identificate con riguardo al disegno ed al funzionamento del Sistema dei Controlli interni relativamente ai Processi sono state documentate;
  - l'attività di verifica dell'operatività e dell'efficacia del sistema dì controllo interno alla data del 31 dicembre 20xx è stata effettuata mediante la valutazione di tutte le inadeguatezze identificate nell'ambito dei Processi;

- che i Controlli, con riferimento alla chiusura dell'esercizio al 31.12.20xx, non presentavano inadeguatezze nei Processi classificate come "significative",
- che i Controlli con riferimento alla chiusura dell'esercizio al 31.12.20xx, non presentavano inadeguatezze nei Processi classificate come "critiche".

dichiaro e attesto

che alla data del 31 dicembre 20xx il Sistema dei Controlli interni relativamente ai Processi era strutturalmente idoneo ed operativamente efficace ad assicurare l'attendibilità dei corrispondenti flussi informativi e il trattamento dei relativi dati in coerenza con i principi contabili applicati dal Gruppo, non presentando inadeguatezze di controllo tali da comportare il rischio di non rilevare e correggere tempestivamente errori o frodi materiali sul Financial Reporting.

Quanto sopra dichiaro non a meri fini interni, ma anche in vista dell'effettuazione da parte della Società di comunicazioni sociali variamente configurate ovvero ai fini del successivo rilascio - anche sulla base della presente dichiarazione - di attestazioni, dichiarazioni e certificazioni suscettibili di determinare profili di responsabilità in capo al dichiarante, a ogni effetto di legge o normativa comunque applicabile.

ESEMPIO 3 - S*CHEMA DI ATTESTAZIONE DEGLI ORGANI DELEGATI DELLE SOCIETÀ CONTROLLATE*

Con riferimento alle istruzioni da voi impartite in relazione al bilancio consolidato [*relazione semestrale*] al 31 dicembre *20XX* [*30 giugno 200X*], il sottoscritto [*Cognome e Nome*], in qualità di [*Consigliere Delegato / Amministratore Delegato / Presidente*], nonché il sottoscritto [*Cognome e Nome*], in qualità di [*Ruolo della persona che rilascia la presente attestazione*] di [*Denominazione Società*] (di seguito "Società"),
premesso che:

- è a conoscenza che il Consigliere Delegato ed il Dirigente Preposto alla redazione dei documenti contabili societari (di seguito "Dirigente Preposto") della Capogruppo debbono attestare, ai sensi dell'art. 154 bis del D. Lgs. n. 58 del 24 febbraio 1998, con apposita relazione allegata al bilancio consolidato, al bilancio annuale ed alla relazione semestrale del Gruppo, l'adeguatezza e l'effettiva applicazione nel periodo (Bilancio 20XX/Relazione Semestrale al 30 giugno 20XX, …) delle procedure amministrative e contabili, la corrispondenza dei documenti contabili societari alle risultanze dei libri e delle scritture contabili, nonché la loro idoneità a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria del Gruppo;

dichiara che, ai sensi dell'art. 154 bis – comma 5 del DLGS 58/98:

I processi di Information Technology individuati secondo quanto previsto nell'ambito del Progetto XXX di Capogruppo, erogati alle aziende del Gruppo sulla base della relazione contrattuale in essere sono adeguate in relazione alle caratteristiche dell'impresa e ai requisiti espressi dai principali framework attualmente riconosciuti a livello internazionale in tema di valutazione dei sistemi di controllo interno (*ad es. CoSO - Committee of Sponsoring Organizations of the Treadway Commission's report e, per la componente IT, IT Control Objectives for Sarbanes&Oxley*), e sono state effettivamente applicate nel periodo (Bilancio 20XX/Relazione Semestrale al 30 giugno 20XX, …). Al riguardo [sono / non sono] state riscontrate problematiche e/o anomalie nel periodo così come evidenziate nella relazione per il periodo allegata.

5.3 Mantenimento della compliance

5.3.1 Introduzione

Negli anni seguenti al primo anno di attestazione il management si trova di fronte alla necessità di mantenere la compliance raggiunta e di gestire la sostenibilità dell'impianto organizzativo e di controllo posto in essere.

In questa fase le principali esigenze che si manifestano sono:

- Verificare che i controlli in perimetro presidino i rischi esistenti anche a fronte di eventuali cambiamenti intervenuti

- Facilitare la progressiva riduzione del costo della compliance

- Incrementare progressivamente la maturità del sistema di controllo

- Mantenere la necessaria focalizzazione della struttura sulla importanza della corretta e costante effettuazione dei controlli IT considerati chiave ai fini della compliance 262

- Facilitare la transizione da una gestione guidata dalla logica di progetto ad una logica di processo

La funzione IT viene normalmente impattata in maniera significativa da questi fenomeni. Tipiche risposte a queste esigenze sono un progressivo incremento del numero dei controlli automatici, un affinamento del perimetro per quanto riguarda entità legali e processi ed una conseguente necessaria revisione dell'ambito IT del progetto.

5.3.2 Situazioni ed evoluzioni

Riteniamo che nel progettare le attività di mantenimento della compliance possa essere utile prendere spunto dalle esperienze maturate nel corso degli ultimi anni dalle aziende coinvolte in progetti simili sia a livello italiano che internazionale e dalle lezioni da esse apprese.
Un elenco non esaustivo di questi suggerimenti con particolare riguardo a quelli che impattano la funzione IT sono elencati nella Tabella seguente.

Situazione	Evoluzione suggerita
La responsabilità per alcune tematiche rilevanti sia per le funzioni IT che per quelle amministrative e di business non risulta chiaramente definita.	La responsabilità per ogni tematica connessa alla compliance dovrebbe essere chiaramente definita. La responsabilità relativa alla “Segregazione dei compiti” ed ai “controlli automatici” non dovrebbe normalmente essere attribuita alla funzione IT ma alle funzioni di business.
La relazione tra il perimetro di intervento ai fini della conformità alla Legge 262/2005 e perimetro (scope) IT non è definito né adeguatamente documentato. Le applicazioni considerate rilevanti ai fini dei controlli IT non sempre sono tutte quelle e solo quelle che dovrebbero essere considerate rilevanti alla luce dello scoping 262.	Best practice in questo ambito sono: - la predisposizione di una idonea documentazione che evidenzi il legame tra società, processo ed applicazione utilizzata - l’implementazione di un idoneo flusso comunicativo atto ad informare

Inoltre modifiche e revisioni al perimetro non vengono tempestivamente ed adeguatamente riflesse nell'ambito IT del progetto 262.	tempestivamente la funzione IT dei cambiamenti operati allo scoping 262
L'attività di compliance IT è focalizzata sulla verifica del disegno e dell'operatività delle attività di controllo	L'adozione di un approccio "top-down" ed una adeguata attenzione alle altre componenti del sistema di controllo interno – in particolare "ambiente di controllo" e "valutazione dei rischi" - possono comportare la riduzione dello sforzo complessivo legato al mantenimento della compliance
Le attività di controllo delegate ad outsourcers non sono state adeguatamente prese in considerazione	Attribuzione di responsabilità interne circa la valutazione del disegno e dell'operatività del sistema dei controlli presso l'outsourcer. Richiesta ed ottenimento da parte dell'outsourcer di attestazioni sul controllo interno (es. SAS 70 Tipo 2)
Le attività di controllo interno descritte e testate nei processi di business sono prevalente mente manuali. I controlli automatici sono evidenziati, descritti e testati in maniera non uniforme nelle diverse società di un gruppo pur in presenza di un parco applicativo uniforme	Una attività centralizzata di razionalizzazione e verifica dei controlli automatici può migliorare il disegno dei controlli e di norma diminuire il costo complessivo della compliance
Tutti i controlli identificati e presenti in azienda sono stati considerati rilevanti ai fini della Legge 262/2005	L'organizzazione dovrebbe valutare criticamente la valutazione dei controlli differenziando quelli rilevanti, per cui è necessaria una attività di testing ai fini della compliance, da quelli non rilevanti. Tale attività genera non solo vantaggi in termini di minori costi ma anche una maggiore focalizzazione della struttura sui controlli più importanti
Mancata adozione di framework riconosciuti (ad esempio COBIT®)	Confrontare le modalità seguite ai fini della compliance con quelle suggerite dagli standard di riferimento e dalle associazioni di categoria. Considerare se l'adozione di un framework complessivo di riferimento possa essere utile anche ai fini di una successiva estensione del perimetro. Questa scelta potrebbe supportare la maturazione delle tematiche di

	controllo interno IT in azienda in vista della adozione di una logica di gestione complessiva della governance IT.
Insufficiente comunicazione tra team responsabili dei processi amministrativi ed operativi e quelli responsabili dei processi IT	Formalizzare i flussi comunicativi tra i vari soggetti aziendali ed organizzare meeting periodici di avanzamento, aggiornamento e condivisione tra dirigente preposto, responsabili della struttura amministrativa e responsabili area IT
Scarsa automazione del processo di compliance	Prendere in considerazione l'utilizzo di applicazioni utili alla formalizzazione del disegno dei controlli ed attività di test e attestazione
Assenza di una gap list centralizzata, inclusiva delle risultanze relative all'area IT.	La creazione di un gap repository centralizzato ed inclusivo di tutte le aree e funzioni aziendali comprese nel perimetro 262, inclusa la funzione IT, consente di valutare in ottica integrata potenziali controlli compensativi ed eventualmente individuare soluzioni centralizzate di rimedio

Tabella 6.2